Unedited version *– Eric Brousseau and Meryem Marzouki*. Internet Governance : Old Issues, New Framings, Uncertain Implications. *in Éric Brousseau, Meryem Marzouki, Cécile Méadel (dir.), « Governance, Regulations and Powers on the Internet ». Mai 2012. Cambridge University Press, Cambridge. Cambridge. ISBN : 978-1107-01342-1. p. 368-397.*

1 Internet Governance: Old Issues, New Framings, Uncertain Implications, by Eric Brousseau and Meryem Marzouki

1.1 Internet Governance: The *What*, *Why*, *How*, *Who*, and *Where*

In the opinion of many actors and commentators, Internet Governance tastes like an old wine in a new bottle—to the extent that some consider, for instance, network neutrality more a matter of co-regulation than of Internet Governance (Marsden 2010). This experience of déjà vu occurs infrequently when we are dealing with network infrastructure and protocols; however, it is widespread when, as throughout this book, we address the regulation of content (Frydman 2004; Marzouki 2008a; Mopas 2009). Even after granting that the Internet is the target and not the means of the governance process,[1] actually delimiting the full scope and complexity of Internet Governance remains a work in progress—as attested by the efforts to define its contours as an academic research field (DeNardis 2010a, 2010b).

Despite its broad definition by the Working Group on Internet Governance (WGIG 2005) mandated during the World Summit on the Information Society (WSIS), the field remains amorphous. The meaning of the term "Internet Governance" varies according to the background and objectives of those who invoke it. The result is many ambiguities and misunderstandings in defining the field and the issues at stake. The differences pertain to all dimensions of Internet Governance, as summarized in the following list.

- The *What*: narrow or broad object? A first set of ambiguities arises with the definition of what, exactly, should be governed. Some would restrict the field to management of critical Internet resources, meaning infrastructure and protocols or, at the least, domain names (Mueller 2002; Paré 2003; DeNardis 2009). Others view Internet Governance as embracing any and all types of regulation—including that of content and behavior—provided only that the object of regulation is somehow related to electronic communications (Benedek et al. 2008).
- The *Why*: particular or general interest? It is generally agreed that Internet Governance decisions affect—directly or indirectly, explicitly or implicitly—all current and future end users, which include individuals, private companies and organizations, and public institutions. However, a second set of ambiguities is related to the intentions and objectives of Internet Governance policies that stem from different visions of the network. Some view the Internet as a commons; it conveys services of general interest and thus should be governed as a public good and with a focus on human rights and democracy (Jørgensen 2006). Others see the Internet as a terrain for technical innovation and economic globalization, which leads to requirements (as driven by a market economy) concerning liberalization of services and fair competition. This

[1] In this sense, Internet governance is a process that differs from e-government in both nature and objectives.

perspective underlies analysis of how power configurations use diplomacy and negotiation to shape the Internet (Singh 2008) and how it is affected by global information and communication technology (ICT) policies (Cowhey and Aronson 2009).

- The *How*: infrastructure, protocol, application, or content layer? A third set of ambiguities regards the level at which Internet Governance applies. Of course, different layers entail different agents defining and implementing such governance policies. Some argue that the core of Internet Governance issues lies in the definition, operation, and political economy of the network infrastructure and protocols (DeNardis 2009). Others concentrate on the role of gatekeepers at application and content levels when defining the means and rules of access to information and communication (Deibert et al. 2008, 2010).
- The *Who*: public or private policy? A fourth set of ambiguities concerns which sectors should be in charge of the Internet Governance process. A report from the International Institute for Sustainable Development (IISD, a Canadian-based policy research institute) argues that it is inappropriate to consider issues that "fall primarily in other public policy arenas" as Internet Governance issues; instead, it suggests calling them "Internet public policy" issues (Souter et al. 2010). However, this claim fails to capture many of the areas touched by Internet Governance or the diversity of the stakeholders shaping the process. Moreover, it fails to acknowledge that the Internet is, for the most part, a privately ordered space and therefore one that must be able to take for granted a pluralistic policing environment (Stenning 2009).
- The *Where*: global, regional, national, or local levels? A fifth set of ambiguities arises when we seek to establish the political settings in which Internet Governance policies should be discussed, adopted, and implemented. The global and interconnected nature of the Internet obviously plays a major role in this discussion. Building on the theories of networked governance and cooperative production by peers, some argue that transnational institutions and forms of Internet Governance are more appropriate than sovereign modes. This perspective eventually leads one to argue in favor of denationalization of Internet Governance as an alternative to the nation-states model (Mueller 2010). Without following the libertarian path, others analyze the different intergovernmental institutions and specialized agencies that have been set up to deal with public policies in the sector (Drake and Wilson 2008). Regardless of the institution or forum addressing Internet Governance, any analysis must treat the legitimacy, transparency, accountability, and inclusiveness of that governance (Weber 2009).

In the end, the extensive range of the *What*, *Why*, *How*, *Who*, and *Where* concerns results in a wide set of interrelated issues. The Internet Governance pie, whether unified or divided, certainly looks even more delectable given the possible combinations of ingredients and their influence.

When a global private organization such as the Internet Corporation for Assigned Names and Numbers (ICANN) decides that the domain name policy should be subordinated to the principles of intellectual property rights (Komaitis 2010), it performs Internet Governance defined in a narrow sense, acting under the influence of some particular interests. When a national public entity such as a government adopts and enforces a legislation criminalizing the

dissemination of child pornography on the Internet, it performs (at the content layer) Internet Governance in a broad sense, acting on behalf of the general interest. In between these two extreme and sharply demarcated examples are a nearly infinite set of intricate issues affecting Internet Governance and thus many areas of individual and collective life. The lack of consensus—as regards not only the specifics but also the scope of what should be done—may be surprising when one considers that more than ten years have elapsed since the United Nations decided to hold a World Summit on the Information Society and five years since the UN actually did so. However, the current situation reflects the drawn-out process of devising a political construct.

This process has been characterized by strong controversies and is certainly not yet complete. In Section 2 we explain how the scope of Internet Governance was widened from mere technical governance to encompass a broader understanding. This process contributed to widening the diversity and number of involved stakeholders, at the cost of the capture of decision making process by those able to master the technicality and the diversity of the discussions, and the implementation of solutions. In Section 3 we examine the major trends evident in the ongoing debates over Internet Governance, thereby demonstrating how this kind of book can contribute to better solutions. We conclude the chapter by resituating the Internet Governance issue in the more general framework of Global Governance.

1.2 Internet Governance As a Political Construct in Progress

The notion of Internet Governance did not emerge in a vacuum. To the contrary, it is largely rooted in long-standing (though still evolving) public policy discussions. However, Internet Governance is much more than a public policy issue in light of four characteristics that capture the essence of the Internet: (i) the interconnection is global; (ii) its management is distributed; (iii) historically, it has been privately coordinated and operated; and (iv) it is intended for the exchange of information and the sharing of capabilities. Other networks, including telecommunication networks, may share one or more of these characteristics, but none exhibits all of them at the same time. This fact grants a unique nature to the Internet Governance process.

1.2.1 From a narrow technical object to a broad political issue

The earliest references to Internet Governance as a tentative political construct dates back to 1998, when two international conferences explicitly named the concept.

The International Telecommunications Union (ITU) 1998 Plenipotentiary Conference in Minneapolis adopted Resolution 73,[2] which instructed its secretary-general to place the question of a world summit dedicated to "the information society" on the agenda of the United Nations. That same year, a conference held by the Internet Society (INET'98) and one by the Computer Professionals for Social Responsibility (CPSR'98) both put Internet Governance on the global political agenda[3]—at least the agendas of the technical community and the civil

[2] All cited UN, ITU, and WSIS documents are available at <http://www.itu.int/wsis>; IGF documents are available at <http://www.intgovforum.org>.

[3] The INET conference series has since 1992 been organized by the Internet Society (ISOC). The Computer Professionals for Social Responsibility is a global civil society organization originally

society. Although the concept of Internet Governance was still unknown to policy makers and business corporations, it had already been recognized and framed by the technical community and civil society groups dealing with information and communication issues.

It is not surprising, then, that the latter two groups—later identified, at WSIS and even more clearly at the Internet Governance Forum (IGF), as "stakeholders"—played a major role in the political construction of the concept. This occurred even though INET and CPSR had different views on the *Why*, *How*, and *Where* and especially on the *What* and *Who*. This difference of perspective and vision has persisted from the early days (in 1998) right up to the Fifth IGF in 2010. In short: the technical community approach to Internet Governance assumes a circumscribed area within which decisions are made by self-regulated technical institutions whose objectives are to "protect the core Internet principles and values";[4] whereas the civil society approach incorporates a much broader scope affecting all fields and necessarily involving the entire range of social actors according to commonly defined rules.

However, this broad conception of Internet Governance by actors in civil society has evolved, in successive WSIS and the IGF proceedings, as a function of the involved civil society groups. The CPSR'98 conference featured a keynote speech by Lawrence Lessig as a preview of his "Code, and Other Laws of Cyberspace" (Lessig 1999), and it held discussions on such topics as "Public Interest in the Age of the Behemoth", "Panic over Privacy: A Case Study in Regulation", "Universal Access: A Global Perspective", and "Convergence and the Internet's Future: Avoiding the Tragedy of the Commons". Even though more than a decade has passed since then, some of these topics remain sufficiently visionary and provocative that they should remain on future IGF agendas.

Yet when the civil society Internet Governance Caucus (IGC) first discussed its terms of reference in 2003, the first draft stated that the group was formed to deal with the "Internet Resource and its allocation governance issues [and] especially the governance structure itself as its starting point."[5] Although the IGC was willing to address multistakeholder participation

---

founded by U.S. computer scientists in 1981; it has incubated a number of projects that led to the formation of some renowned organizations and conferences, such as the Electronic Privacy Information Center (EPIC) and the Computers, Freedom and Privacy (CFP) conference series. Information and documents on the INET'98 and CPSR'98 conferences are available online at <http://www.isoc.org/inet98> and <http://cpsr.org/prevsite/onenet>, respectively.

[4] It is interesting that a new, "dynamic coalition on core Internet values" was formed at the 2010 IGF. Its launching workshop description includes the following statement: "The Internet model is open, transparent, and collaborative and relies on processes and products that are local, bottom-up, and accessible to users around the world. These principles and values are threatened when policy makers propose to regulate and control the Internet, with inadequate understanding of the core values." (Full text is available online at <http://igf.wgig.org/cms/dynamiccoalitions/90-dc-meetings-2009/481-dynamic-coalition-on-core-internet-values>.)

[5] From the first message sent to the IGC mailing list by the then caucus coordinator on 1 April 2003. Mailing list archives are available at <http://lists.cpsr.org/lists/arc/governance>. The IGC is a loose coalition of civil society organizations and individuals formed during the WSIS at the same time that other civil society thematic caucuses were created. After the WSIS resumed and the Internet Governance Forum was created as a follow-up process, the IGC became the de facto unique representative of civil society at large. More details are available from the IGC website: <http://www.igcaucus.org>.

in Internet Governance structures, it sought to restrict that participation to Internet technical resources management structures and, in particular and primarily, to the Internet Corporation for Assigned Names and Numbers. The IGC accordingly restricted itself to a narrow definition of the Internet Governance concept. At that time, other issues were handled by the numerous other thematic caucuses formed by civil society at WSIS.

Discussions among government representatives have witnessed the same evolution with regard to a narrow versus broad understanding of Internet Governance. As documented in the literature (Raboy et al. 2010), by the end of the WSIS's First Phase, the battle over Internet Governance was focused on the internationalization of domain names and other critical matters of Internet resources management policy. At this point there were almost irreconcilable positions of unilateralism (the U.S. government, through its contract with ICANN) and multilateralism (the UN governments, through the ITU). The long, heated, and nearly epic discussions ended diplomatically with creation of the Working Group on Internet Governance, which was charged with the task of defining Internet Governance and the policy issues surrounding it.[6] Paragraph 50 of the WSIS Geneva Declaration of Principles explicitly calls for the creation of this working group. Although the WGIG's name includes *governance*, it's only *management* of the Internet that is mentioned in the Declaration's two immediately preceding paragraphs. Paragraph 48 highlights the need for an equitable distribution of the Internet's resources, for its stable and secure performance, and for multilingualism to be taken into account. Paragraph 49 lists all the actors that need to take part in this process—namely, the four recognized WSIS stakeholders. These stakeholders acknowledged that both technical and public policy issues were at stake, but it remained their intention solely to *manage* the Internet and its critical resources.

It was only after the wider definition espoused by the WGIG report—and after formation of the IGF as one of the WSIS follow-up forums—that the understanding of Internet Governance broadened. The WGIG defined an extensive set of issues encompassed by Internet Governance, ranging from the "administration of the root zone files and system" to "capacity building" and the "meaningful participation in global policy development" as well as a whole set of human rights and consumer rights issues directly at stake in the governance of information and communication processes. From the civil society perspective, then, the IGC had widened its scope according to this broad definition of Internet Governance and accordingly expanded its membership to include civil society participants who were previously involved in other thematic caucuses. From the government perspective, the WGIG report was welcome but the fundamental issue of control over critical Internet resources—which was viewed as a matter of state sovereignty—remained unresolved even by the end of the WSIS Second Phase. Arguments over this issue led to frontal opposition between the unilateral and multilateral visions that lasted up until convening of the Tunis Summit.

The confrontation was provisionally resolved by the following two simultaneous decisions. The first was to convene the IGF as a post-WSIS "new forum for a multi-stakeholder policy

[6] An account of WGIG history, composition, and outcomes is available from WGIG website: <http://www.wgig.org/index.html>.

dialogue" as set forth by the mandate in Paragraph 72 of the Tunis Agenda. The other was to initiate a process of "enhanced cooperation", as defined in Paragraph 69, "to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues."

This split decision was the WSIS's "answer" to both dilemmas—unilateral versus multilateral and technical versus political—of Internet Governance.

1.2.2 From NWICO to WSIS: Revisiting an old conflict

Whether defined in a narrow or a broad sense, Internet Governance emerged as one of the leading issues of the WSIS Second Phase (2003–2005) mainly as the result of civil society action.

The WSIS evolution was indeed so unexpected that many commentators identified two paradoxes about the summit (Raboy and Landry 2006). The first paradox concerns the World Summit's organization by the ITU instead of the United Nations Educational, Scientific and Cultural Organization (UNESCO), which was considered a more appropriate agency to take the lead on information and communication issues. The second paradox is the choice of Tunisia as the venue for the WSIS Second Phase. Many considered it an intolerable affront to hold a summit on information and communication in a country whose citizens were notably muzzled at that time. However, both alleged paradoxes mainly proceed from erroneous analysis: they ignore the historical antecedents of the WSIS. In fact, the choices of ITU and Tunis are linked. The idea of a high-level international meeting aimed at "reducing the digital divide" was indeed proposed by Tunisia at the 1998 ITU Plenipotentiary Conference in Minneapolis, which adopted this principle.

The original proposal was fully coherent, since the meeting's purpose was to discuss and find solutions to the global issues of deploying and financing the infrastructure for digital networks and, in particular, the problem of international interconnection costs and of interconnection agreements between intercontinental network operators (Abramson 2005; Badasyan and Chakrabarti 2005). Thus, in line with a concept of the "digital divide" that was limited to infrastructure issues and with a technocentric vision of the "information society", these choices were not devoid of rationality. The ITU was an appropriate UN agency because it had declared itself (in its 1998 Resolution) to be "conscious of the emergence of the concept of the information society in which telecommunications play a central role." For similar reasons, Tunisia was a developing country no less legitimate than any other as a venue for this summit (Jørgensen and Marzouki 2005)—provided one sticks to a technical vision of the information society as the ITU apprehend it (Ksibi 2006).

However, the idea turned from an ITU-level meeting for addressing operational objectives into a much more ambitious proposal for a World Summit on the Information Society, adopted by the United Nations General Assembly in December 2001. At about the same time, in fact, the UN adopted its Declaration of the Millennium Development Goals (MDGs); these goals established a series of objectives covering a wide spectrum of areas that included peace efforts

and strengthening of the UN as well as human rights, democracy, and good governance.[7] Via this Millennium Declaration, member states had already committed themselves to "ensure that the benefits of new technologies, especially information and communication technologies are available to all." Although the concept of an "information society" was not mentioned, its main elements—an "emancipatory" vision of technical progress and an instrumental vision of the "information society"—were emphasized. It should be noted, though, that the reference to "new technologies" was actually made only as a means of achieving the Declaration's goal of "development and poverty eradication".[8]

Nonetheless, WSIS frequently refers to the Millennium Declaration and the MDGs in their entirety. In 2002, for example, the Marrakech ITU Plenipotentiary Conference identified as one of WSIS goals the need to achieve the Millennium Development Goals. During the subsequent WSIS process, these goals have often been recalled by all stakeholders as key WSIS issues, motivations, decisions, and actions. The four official WSIS documents[9] thus mention the MDGs in great detail but always with an eye toward promoting a "Brave New Digital World" (Leuprecht 2005). The WSIS civil society Declarations of 2003 and 2005 also channel the MDGs but from a less technocentric perspective.

This unexpected extension of the original scope of the conference—in particular, by reference to the entirety of the MDGs—introduced to WSIS the very ambiguities conveyed by the notion of "information society". It was thus no surprise that, during its First Phase, WSIS experienced the revival of a 30-year-old conflict that originally arose during discussions on the New World Information and Communication Order (NWICO) at UNESCO during the Cold War.

Since that time, the central question of regulating information exchanges and communication had remained unresolved even as it became more crucial with the explosion of technologies and a global economy—factors that gave the question an even more complex dimension. On the one hand, the post–September 11 "war on terrorism" questioned, even in Western democracies, the necessity of complying with principles of human rights and rule of law. It highlighted also the crucial nature of the so-called Information War. On the other hand, the means of communication were no longer "concentrated in a handful of countries" (a circumstance decried by the Non-Aligned Movement in 1976) because the political and economic landscapes had been dramatically transformed by the emergence of new economies and the strengthening of formerly weak nation states. Furthermore, in a world with the Internet, governments are not the sole gatekeepers. The control of global communication

[7] More detailed information on the UN Millennium Declaration and the Millennium Development Goals is available at <http://www.un.org/millenniumgoals>.

[8] The Eighth Millennium Goal is to develop "a global partnership for development" by (among other things) "co-operation with the private sector, mak[ing] available [to all] the benefits of new technologies, especially information and communications." The indicators defined by the UN to assess progress toward this goal were simply two classical, "per 100 population" ITU indicators: (i) the number of telephone lines and cellular subscribers and (ii) the number of personal computers and Internet users.

[9] The Geneva Declaration of Principles and the Geneva Plan of Actions of 2003 and the Tunis Commitment and the Tunis Agenda for the Information Society of 2005.

infrastructure and hence of information flows has become distributed among many de facto regulators.

Thus, the same lines of conflict as during NWICO discussions now appeared between promoters of development and those primarily attached to the establishment/preservation of fundamental liberties, and the same old arguments were rehashed (Hamelink 2005). Veterans of the McBride Roundtables,[10] including members of the Communication Rights in the Information Society (CRIS) campaign, were thus opposed to media groups and associations promoting freedom of expression. The former were brandishing a "right to communicate", which was eventually reframed as "communication rights" (Jørgensen and Marzouki 2005; O'Siochrú and Alegre 2005); the latter were promulgating a "free flow of information" doctrine (Koven 2003). The protagonists remained the same at the governmental level also, as if there had been no historical, political, economic, or technological evolution in 30 years. This conflict, which had already proved sterile during NWICO times (Mattelart 2000), has once again prevented WSIS from any attempt to discuss and rebalance unequal terms of exchange in the information and communication sector.

1.2.3 Governing an information society without defining its polity

The World Summit on the Information Society failed to resolve the very questions that led to its convening—that is, managing the network infrastructure and financing. Here again, an explanation can be drawn from the participation of the civil society.

The Second Phase of the WSIS took a different shape from the First Phase, as there was a major change in the typology of civil society participants (Marzouki 2008b). Some groups (e.g., key members of the CRIS campaign) moved away, seeing little hope within this framework to advance their specific objectives, which focused on the right to communicate. They chose instead to concentrate their efforts on issues germane to their concerns and capacity of action. Toward this end, these groups switched to the UNESCO arena; here discussions were ongoing in anticipation of adopting the Convention on the Protection and Promotion of the Diversity of Cultural Expressions.[11] The publicity surrounding the Geneva Summit had raised the interest of organizations active in sectors as diverse as the Millennium Development Goals themselves and carrying the same instrumental perspective of the information society as the one advocated in the WSIS definition. It also led to increased involvement by individual participants. In particular, academics and consultants joined WSIS on the basis of their specific interest in Internet Governance. This was especially true for many members of the technical community and also for political scientists. The trend is most notably attested by the composition of the Working Group on Internet Governance and by the related intense publication activity during this period under the auspices of international organizations (MacLean 2004b; Drake 2005; Stauffacher and Kleinwächter 2005).

During WSIS's First Phase, the diversity of civil society actors and of their interests and

[10] More information on NWICO actors and the McBride Roundtables are available on this resource's website: <http://www.nwico-wsis.net>.

[11] More information on this convention, which was adopted in 2005, is available on the UNESCO website: <http://www.unesco.org/new/en/unesco/themes/2005-convention>.

claims did not prevent them from reaching a consensus on some sectoral issues, mainly through a juxtaposition of specific and not antagonistic claims against positions of governments and of the private sector. However, points of conflict soon emerged among civil society actors over three main issues: multistakeholder partnership and Internet Governance (McLaughlin and Pickard 2005), human rights (Marzouki and Jørgensen 2005), and the financing of infrastructure (Peyer 2005). Clearly, these issues are less related to stakeholders' identities than to political choices.

The WSIS Second Phase had fewer conflicts in terms of substance but also fewer asserted positions. The dullness of the 2005 Civil Society Declaration is indicative of changes in the type of civil society involvement from one summit phase to the other. This dynamic can be explained by three factors, which are related to the three contentious issues that arose during the First Phase.

First, many nongovernmental organizations (NGOs) involved in the defense of human rights focused, during the Tunis Phase, on the bad record of the country regarding freedom of information and communication. Hence observation missions, meetings, and organizing other public events were at the core of NGO activity during this Second Phase. Tunisia's bad reputation has even hijacked the PrepCom proceedings.[12]

Second—and this is the main explanation—Internet Governance and multistakeholder partnership were the focus of an ad hoc working group (the WGIG). Discussion of these issues, which was actually confined to this restricted arena during WSIS's Second Phase, led to creation of the global Internet Governance Forum. The IGF was thus established under the auspices of the United Nations by the Tunis Agenda and Plan of Action; indeed, it was mandated to meet regularly in order to implement Internet Governance according to the principles, processes, and procedures defined by that agenda. Hence the IGF has been, since 2006, an annual international meeting that serves only as a discursive space to facilitate a "global conversation". In particular, the IGF does not allow itself to make any decision or offer any recommendation; it thereby ensures its survival, which is constantly threatened by the power game between states (Malcolm 2008). For instance, China and the Group of 77[13] threatened not to renew the IGF's five-year mandate in 2010.[14]

Third, the financing of infrastructure was the topic of a different ad hoc working group whose final report raises more questions than it answers and has seen no follow-up. A global Digital Solidarity Fund (DSF) had been created at the end of the Geneva Phase and was formally

[12] This was especially true with the Hammamet PrepCom in June 2004, as reported by the WSIS Civil Society Human Rights Caucus; see <http://www.iris.sgdg.org/actions/smsi/hr-wsis/tunis.html>.

[13] The Group of 77 at the United Nations, also known as the Non Aligned Movement, is a loose coalition of developing nations, designed to promote its members' collective economic interests and create an enhanced joint negotiating capacity in the United Nations. There were 77 founding members of the organization, but the organization has since expanded to 131 member countries. The group was founded on June 15, 1964 by the "Joint Declaration of the Seventy-Seven Countries" issued at the United Nations Conference on Trade and Development (UNCTAD).

[14] See e.g. transcripts of IGF sessions at <http://www.intgovforum.org>.

approved at the conclusion of the Tunis Phase. Yet in acting mainly as a patronage tool, the DSF amounts to little more than a private foundation. It can therefore hardly be seen as a substitute for policies that aim to develop Internet infrastructure and access. It mainly supports projects based on information and communication technologies.[15] To date, the DSF has failed to promote effectively its principle of a "1% digital solidarity tax" as a source of financing. This "tax" would consist of successful tenders in public projects related to ICTs *donating* to the DSF 1% of the transaction value, a fee meant to be deducted from their profit margin. Although some local authorities have signed up, this mechanism is struggling to find a critical mass of support and must still convince doubters of its relevance in political terms and especially in legal terms (Weber and Menoud 2008).

Given these developments, the WSIS ended without resolving two of the main issues that this United Nations World Summit sought to address: the financing and governance of the Internet. So even though an "information society" has been enshrined by the UN, the concept lacks definition not only of its organization fundamentals but also of its conditions of access and participation in this "society" and the articulation of powers that govern it.

1.2.4 From organized civil society actors to policy entrepreneurs

The sidelining of organized civil society actors is another consequence of these developments at WSIS. This is most probably a long-term trend, since it has been reinforced in the post-WSIS framework of the IGF from 2006 to 2010.

It is common knowledge that the WSIS proceedings included neither trade unions nor antiglobalization social movements nor most of the NGOs that traditionally structure civil society participation in major intergovernmental conferences and world summits; what's puzzling is why these excluded groups showed so little interest in the WSIS (Marzouki 2008b). This lack of understanding of WSIS political stakes was complemented by blindness about the transformations that might have resulted in terms of how the civil society representation was organized.

Furthermore, the post-WSIS phase has witnessed the sidelining of most organized civil society players, especially those that formed coalitions and caucuses during WSIS. This shelving—to which, it seems, most of them consented—led to participation by only a handful of civil society organizations, rather than large coalitions, and to most individuals acting on their own. This generalization applies, at least, to the dominant shape of the civil society Internet Governance Caucus, which became the forum for gathering and representing civil society in the post-WSIS phase. This trend strengthened with the Internet Governance Forum, which was created by WSIS as a follow-up to the WGIG.

The WGIG had proposed a definition of Internet governance that reflected a much wider perspective than managing the system for domain names. Indeed, this definition refers to 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 programs that shape the evolution and use of the Internet." Thus are included not only the governance of

[15] As is evident from the DSF website: <http://www.dsf-fsn.org>.

critical resources needed to ensure the network's proper functioning but also the governance of its uses. Moreover, this definition speaks to multistakeholder governance and not to political regulation by governments alone.

A greater involvement of actors other than governments—most notably, of civil society organs—in the management of world affairs is, naturally, a welcome development. However, such multistakeholder governance does raise some democratic issues. When coupled with a trend to deal with any and all Internet-related public policy issues, it might result in an arena immune to the rule of law. The risk is that such governance arrangements need not comply with international protections for human rights (since only governments are bound by these standards) and thereby dilute the responsibilities of states and their accountability to citizens. In its own report, the WGIG highlights that it "comprised 40 members from Governments, private sector and civil society, who all participated on an equal footing and in their personal capacity." The WGIG limited its task to identifying different, even contradictory approaches to Internet governance without deciding in favor of any of them. Yet the IGF's having reproduced the WGIG modus operandi in itself raises democratic concerns, since the latter's mandate extends to "discuss public policy issues related to key elements of Internet governance".

The WGIG definition of Internet Governance, as adopted by WSIS in 2005, refers to the same general object as do widely agreed definitions of governance. For example: "Governance is a term that applies to the exercise of power in a variety of institutional contexts, the object of which is to direct, control and regulate activities *in the interests of people as citizens, voters and workers*" (Robinson 1996; emphasis is ours). And: "Governance may be defined as a process of coordinating actors, social groups and institutions, in order to achieve collectively defined and discussed objectives. Governance refers then to the set of institutions, networks, guidelines, regulations, norms, political and social usages, as well as public and private actors *contributing to the stability of a society and polity, to its orientation, to the capacity to conduct affairs, to provide services and to ensure its legitimacy*" (Boussaguet et al. 2004; translation and emphasis are ours). However, fundamental components are missing in the WGIG definition—namely, the governance objectives and the governed polity. In other words, the Internet Governance definition, as established since WSIS and supported through five years of the IGF process, remains instrumental only: although it covers the *What* and the *How* and, to some extent, the *Where* of Internet Governance, it is sorely deficient in addressing the *Why* and *Who* components.

Civil society actors, from WSIS to WGIG to IGF, have played a major role in defining Internet Governance as a political construct, and the viability of this concept is evidenced by the high degree of interest it has raised in the academic literature. This literature typically analyzes civil society participation in terms of NGOs and other civil society *organizations* (Cammaerts and Carpentier 2005; Raboy and Landry 2006) or in terms of *individuals* (Lakel and Massit-Follea 2007; Pavan and Diani 2008; Cammaerts 2010), but researchers have not analyzed the evolution of participation from collective to individual civil societies. We have shown that detailing this evolution sheds light on the political consequences of the progressive delegitimization and/or disqualification of organized social actors. Indeed, doing so illuminates how the various civil society stakeholders understood and built expertise, in matters of Internet

Governance, that reflected their visions, interests, and the game they played. Some empirical analyses have shown that establishment of the IGF, its advisory committees, and its rules of procedure have reinforced the participation and influence of various "experts" (academics and consultants) to the detriment of NGOs, trade unions, and social movements (Raboy et al. 2010). So-called policy entrepreneurs (Kingdon 1995) thus found their window of opportunity in the context of a weakened role of the state (Marzouki 2008b).

1.2.5 The uncertain implications of a new governance territory

The transformation by which civil society perceived and presented itself as one of the three Internet stakeholders (with governments and the private sector as the other two) should also be analyzed through the prism of an *individual*-centric vision of society, as theorized by Hegel building on the Scottish Enlightenment philosophers. The Gramscian perspective, which identifies "civil society" as an organized and autonomous sphere independent from the market and the state, may indeed no longer be relevant in light of the concept's actual evolution.

In fact, "communication rights" were at the heart of heated debates during the WSIS First Phase (2002–2003), due most notably to the involvement of organized civil society actors (CRIS Campaign members, Civil Society Human Rights Caucus members, Media Caucus members) with strong and diverging viewpoints on how those rights should be defined. Research linked to the WSIS Second Phase (2003–2005) shows—and research subsequent to establishment of the IGF confirms—that there has been a regression in prominence of the concerns related to socioeconomic and development or *collective* rights. Evidently, consensus can be reached only on *individual* rights such as freedom of expression and privacy. These developments are obviously in line with declines in traditional forms of representative democracy and with the crisis faced by nation-states in the context of globalization.

These transformations might pave the way to new global governance if not a new world order, and some see this as an opportunity to reduce further the role of governments (Mueller 2010). In any case, the evolution of civil society strongly affects our definition and understanding of human rights, democracy, and the rule of law. In such an unstable transition period—while the state's role is being reconfigured from that of the "welfare state" to the "regulatory state" or even, as advocated at the national level by the New Public Management philosophy and practices, to simply the "steering state" (Bezes 2009)—governance developments might lead to uncertain implications, especially in the digital "territory" characterized by a high diversity of powerful gatekeepers and de facto regulators. Moreover, the nonconclusive nature of the debates in many arenas, and especially within the IGF, should be contrasted with the operational pragmatism of those instances where de facto governance principles were implemented—often behind the veil of simple technical regulation, as is well illustrated by ICANN. Internet governance is, indeed, developing.

1.3 De-territorialization and Re-territorialization of the Internet

The current institutional framework is characterized by inconsistencies, overlapping domains, missing links, and most of all a constant evolution. Nonetheless, Internet Governance is de facto operating and framing the process of that evolution. Three main issues dominate today's

debates: the risk of fragmentation, the network's degree of openness, and protection of data. We shall review each of these issues in turn.

1.3.1 A threat of rampant fragmentation, beyond democratic and legal control

It has been pointed out in several chapters that the digital world's imaging of the actual one is increasingly characterized by the notion of *heterarchy*. All kinds of gatekeepers (technical intermediaries, community leaders, public agencies, services providers, etc.) emerge and tend to impose restrictions on use of the network by systematizing the control of information exchanges and access to services. The threat is clear: the Internet could rapidly split into a set of interconnected information networks controlled by commercial and governmental gatekeepers. The price of this development would be a decrease in global integration of the networks and an attendant massive loss of information and positive network externalities—regardless of the extent to which it protected the citizens'/users' freedom and privacy.

The present fuzziness in the process of building a satisfactory global governance framework favors this path of evolution. Indeed, governments and commercial interests have made loud calls for "pragmatic" solutions to a set of particular issues (including criminal activities, property rights infringement, threats to security, protection of trade secrets, etc.). Even the protection of citizens' fundamental liberties might lead to a call for the building of digital fences. Note that control of access, procedures of identification, and filtering of content have already been combined so that Internet and mobile service providers can manage access to services on an individual basis. The logic is both economic and politic. On the one hand, most commercial service providers are interested in technologies that will enable them to implement digital tolls while preventing leaks or misappropriation of information services. On the other hand, public authorities have an interest—which can be enhanced by public opinion—in fighting what they consider to be abuses and criminal uses of the Internet. The result is either development of public control capabilities or pressures on providers of information and Internet service. This dynamic explains the persistent trend of fragmentation by which the end-to-end character of the information infrastructure is strongly decreasing.

Whether or not the public and private attempts to control Internet use prove successful is actually a secondary issue. In any case, it is the generalization of these measures that leads to a decrease in global connectivity and to an increase in the complexity (and costs) of using the information infrastructure. Such a trend leads to diminished capabilities of sharing information and knowledge but reinforces the status quo of market and political powers. Moreover, since uncertainty might well hinder innovation and investments, the true "conservative" dimension of these movements must be emphasized. Whether led by governments or corporations, their goal is to restore the past order. Governments seek to recover their sovereignty and ability to regulate access to and exchanges of information. Corporations seek to enshrine their past business models, as illustrated by entertainment industries preventing free access to content; these industries would rather implement pay-per-view or subscription-based systems than consider alternative business models that could still remunerate creation but also increase creative diversity. In both cases, the full economic and social potential of digital technologies is not explored because, in part, most of the discourse is concerned with fending off perceived threats to survival.

Two phenomena must be mentioned as having a large impact on the evolution of digital matters. First is the relatively recent trend of international governance based on voluntary adhesion to non mandatory norms. Because consensus is hard to achieve among stakeholders and especially (owing to divergent national interests) among governments, new norms tend to be developed on a voluntary basis within forums. In accordance with the procedures of ICANN and related organizations, these norms are elaborated cooperatively among industries, high-profile governments, and the most active stakeholders. An example is the Anti-Counterfeiting Trade Agreement (ACTA), initiated in 2008 and formally launched in 2010, which seeks to establish international standards for the enforcement of intellectual property rights enforcement. This agreement would establish a new, *international* legal framework, which countries could join on a voluntary basis, and its own governing body that would not be subordinate to any existing institutions. The aim is to standardize and coordinate enforcement policies and to develop, when needed, more adequate national capabilities. Clearly this effort is a response to what the most developed countries view as an essential threat: the huge numbers of counterfeit goods and ever-increasing instances of copyright infringement. The scope of ACTA includes counterfeit goods, generic drugs, and copyright infringement on the Internet. The plan is to organize an agreement among some OECD countries and then to convince emerging economies that they should sign on (Yu 2011)

The other trend is the "mission creep" evidenced by those agencies or international agreements that succeed in addressing an issue. Their promoters are then often tempted to extend the scope of their initial mission on the basis of the legitimacy and capabilities accumulated during an initial phase that addressed a legitimately agreed-upon issue. For instance, the strong desire to expunge criminal activities could easily be used to justify implementation of oversight capabilities with respect to all exchanges of content; clearly, this would increase the likelihood of infringing on freedom of expression and privacy rights. It is also well known that, once created, organizations tend to expand their activity beyond their initial goals—if for no other reason than because members and various stakeholders have an interest in the organization's continued existence. That Internet service providers (ISPs) developed hotlines for reporting about child pornography is an example of mission creep. In fact, many of them are now relied upon to encourage exposure of extended lists of abuses.

Both trends make it clear that the development of new regulations, often under the shadow of governments, tends to escape the control of democratic and legal institutions. Most often it is a question of sophisticated implementation technologies discussed by closed groups of high-level bureaucrats, engineers, and public and private decision makers, whose compliance with democratic and legal norms are difficult to assess. Furthermore, pragmatism often requires quick decisions, even though international agreements tend to create (sometimes unfortunate) irreversibilities. Ex post demands for conformity are weak and probably hopeless given that actual technical implementation results in de facto adoption and thus stimulates imitation of the existing (albeit imperfect) solutions. Thus, the *fait accompli* tends to be a central characteristic of this trend toward fragmentation.

This is why pockets of resistance persist. Cryptographic resources and peer-to-peer (P2P) networks are mobilized by groups of activists to reduce the likelihood of external control. A

good illustration of such "technological" defense is the TOR project, whose aims include hindering identification elements when a user accesses the Internet as well as disseminating exchanges of information in order to circumvent surveillance efforts.[16] A parallel course is taken by human rights activists who attempt to identify potential threats and to influence the process of norms making: by involving themselves in international discussions (in particular, those of the IGF); by lobbying ministries, regulators, and parliament members at the national and regional level; and/or by suing governments and corporations responsible for implemented solutions that infringe on citizens' essential rights.

Beyond those losses in terms of the global information infrastructure's potential, the current trend of fragmentation might also lead to a major political reordering. In this case we could lose the potential of innovative principles of collective regulations, and the resulting order could well lead to a regression in which the hierarchy of norms is weakened at all levels and replaced by the coexistence of unarticulated norms and in which the democratic control over their elaboration and implementation is more difficult. Such control has never been universal but was the dominant paradigm in most developed countries after World War II. The endpoint of this trend line would be consistent with what some specialists in international relations refer to as "new medievalism" (Bull, 1977; Friedrichs, 2001; Spruyt, 1994).

1.3.2 Neutrality in managing access and flows

To a large extent, the fragmentation debate overlaps with the one over "net neutrality" (NN). Yet we should continue to differentiate the two issues because they do not concern the exact same issues and dynamics. The fragmentation debate clearly involves network content and the control of information flows, whereas the NN debate is related to the fundamental dialectic of network management and is therefore more concerned with the actual data flow. On the one hand, the Internet relies on the renowned "end to end" principle whereby the network's role is to serve as passive intermediary among active terminals. Under this principle, all content, sites, platforms, and users are considered equal in terms of how the network and its communications are managed.

The end-to-end principle is the very source of the network's flexibility because (i) it favors interconnection among heterogeneous networks and (ii) it enables sustained implementation of innovation in services by connecting new equipment and software to the network. On the other hand, quality of service cannot be guaranteed without the technical management of flows when congestion occurs. Remedies may be based on queues but also on rerouting, discrimination among flows, or even incomplete transmission of certain packets. The ISPs have limited capacity and the volume of data transported on the Internet is skyrocketing, so telecom operators and access providers increasingly employ traffic management software to streamline their networks, prevent congestion, and promote value-added services. The latter generally require management of priorities within the network to ensure that bandwidth-demanding flows are delivered on time and to guarantee the integrity and security of access and of information exchanges.

[16] More information on the TOR project is available at <http://www.torproject.org/>

Hence the network neutrality debate has two dimensions. The first is that of discrimination among flows, and it raises mainly technoeconomic issues related to the nature of competition within the network. The key issue is whether the ISP should be allowed to discriminate among other service providers on the basis of commercial preferences and payment. This debate echoes the one that developed in the 1980s about the neutrality of so-called common carriers. Then and now, the central questions are *who* should pay for development of the infrastructure and, if bandwidth is scarce, *on what basis* should access be provided. The question of payment pits the information service providers (especially those of the Web 2.0) against ISPs and "backbone" providers. The latter would like to charge the information service providers for the increased traffic that they generate. In response, the former argue that their information services are what allow ISPs to market and sell high-speed access to the final users and thereby generate revenue for financing the infrastructure. The question of access pits ISPs against the most advanced and intensive users. Indeed, ISPs could easily solve their capacity constraints by downgrading the quality of service to targeted uses or users. They might also employ this capability to throttle certain flows while promoting their own services (examples include online telephony, music, and video) or those of their allies. More broadly, network management practices tend to favor (centralized) servers and information service providers whereas strict neutrality with respect to bandwidth demand would favor (dispersed) end users and peer-to-peer practices. Yet for one mode to prevail would mean unfair discrimination—among either users or service providers, with possible abuse of a dominant position in the latter case.

The second dimension of the NN debate is that of content filtering, which raises issues related to freedom and fundamental rights. The key issue here is whether the ISP should be allowed to perform "deep packet inspection" and possibly block targeted traffic (Daly 2010, Bendrath and Mueller 2010) On the one hand, this might be justified in terms of service quality, which improves if the ISP can block junk mail, defuse viruses, and block cyberattacks. On the other hand, these capacities could be used to repel certain norms (and thus to advance others), both legal and moral. The point is that, once they can filter content, ISPs (and, more generally, information service providers) might well be pressured to block content disliked by some authority or organized group. Most agree that legal authorities can legitimately rely on ISPs to help enforce certain legal norms, as in cases of transmitted child pornography or other criminal activity. However, few would support a government's hindering the ability of opponents to access and exchange information, a religious group's attempt to impose their moral norms, or the blocking by economic interests of access to information about their operations.

With the following matrix we attempt to clarify matters by distinguishing the two separate "levels" of the debate that are often conflated in public discourse and the media. Although filtering and discrimination might well be justified in the service of technically optimizing the infrastructure's capabilities while maintaining its fundamental neutrality, the same techniques can bias the competition among information service providers toward those allied with the ISPs and also lead to the exercise of political power without any guarantee of legitimacy.

Purpose \ Object of Filtering	Data Flows	Content
Quality of Service	Optimization of bandwidth use (especially when synchronization is needed)	Assurance of quality, reliability, and security
Use of the Network	Discrimination among alternative services and providers	Control to block access and to block the exchange of targeted contents

The position of the various stakeholders is often complex in these debates. For instance, ISPs would probably prefer being allowed to discriminate among flows because doing so would allow them to charge information service providers for the traffic they initiate. Moreover, they would likely also be pleased to promote their own services and those of their allies. At the same time, ISPs are strongly disinclined to filter content, not only because it would be costly to implement but also because it could make them liable for violations of intellectual property rights or of any other public regulation. Citizens are probably most concerned about their use of the Internet being controlled by an ISP, although they would value any operations performed by the ISP to enhance the quality of service. Political authorities and interest groups would naturally value the ability to filter content toward the end of promoting compliance with their various norms. Economic interests—except for those (e.g., the major entertainment industries) that would ally with ISPs—would much prefer that ISPs *not* be able to discriminate among data flows. It should be clear that a strict application of the NN principle promotes a "political" vision of the network as an essential resource that should be available, without restriction, to everyone; in this view, the question of how to finance the infrastructure's development is less important. Thus the NN vision contrasts with a more technoeconomic view that admits traffic management is required given a limited infrastructure that must necessarily be optimized.

In different countries, debate on how to deal with the NN issue has resulted in sensibly different regulatory frameworks for Internet Traffic Management Practices (ITMPs). More important, though, is that existing frameworks are still evolving and hence ISPs may later face alternative regulations—whether they are distributing services on the basis of a cable, telephone, or Hertzian network. As pointed out by Stevenson and Clement (2010), the prevailing practice in developed countries is to limit ITMPs as much as possible and to relieve network congestion by encouraging the development of infrastructure. When they are allowed, ITMPs should be transparent to users. The reason is that such practices might be problematic: from a technical point of view, because they might hinder innovation; and also from a social perspective, given their potential negative political and economic consequences. Broadly speaking, ITMPs have no supportive constituency but are seldom forbidden outright.

The countries that allow operators to employ ITMPs typically rely on competition among network providers to control possible drifts.

It is worth mentioning that, at the international level, the NN debate is echoed by the question of asymmetrical peering agreements between the North and the South. Because most of the bandwidth and information resources originate in the most developed countries, access to the global information infrastructure by ISPs located in developing countries (and especially in the least developed countries) is priced at a very high level. In short, Southern users want to be connected more than Northern providers want to connect them. This imbalance is reflected in the high cost of Internet access for Southern users, who also suffer from poor quality of service because the South's infrastructure has not been (and, perhaps, cannot be) fully developed. The persistence of asymmetry in peering agreements is one of the factors hindering establishment of an advanced information infrastructure in developing countries, and it reinforces the digital divide between North and South.

1.3.3 Privacy and identity

One of the characteristics of the Web 2.0 is its new approach to the relationship between individuals and collectives. On the one hand, as illustrated by online social networks, individuals voluntarily share private information with others on a relatively wide scale. In so doing, they have shifted the traditional boundaries between private and public life, staking out an ever-larger space of hybridization between the two. On the other hand, as illustrated by P2P networks and cloud computing,[17] individuals also opt for systems that enable them to share computing capabilities and information resources on an automated and relatively anonymous basis. Such behavior blurs the traditional frontier of property rights: They no longer allow the ability to control what uses are made of one's personal data and property or to discriminate among those seeking access to confidential or proprietary information.

These divergent paths of evolution—which mainly reflect the behavior of individuals (who do not always anticipate the consequences for their own privacy, rights, and security)—have a parallel in those advocated by governments and corporations. The desire to reestablish sovereignty over network activities or (respectively) to secure business models leads to the development of technologies that aim to identify and track individual activities. In neither case is the intent to act systematically and purposefully against citizens. Yet because they are responsible for the general interest and welfare, governments legitimately seek to fight crime, to avoid fiscal and other anticivic evasion, and to ensure the security of citizens and of essential collective infrastructures. Firms also act legitimately when they seek to preserve the collective investment of all stakeholders by preventing leaks of industrial and trade secrets or to secure remuneration for the services they provide. (We remark also that customized management of information about consumers/users could be of value to all concerned parties.) These considerations have led to the development and deployment of myriad technologies (e.g., video surveillance, tracking of card and phone use, geolocalization, control of access,

[17] In the case of cloud computing, it is most often the IS manager who decides whether or not to opt in; with P2P the decision to opt in (and out) remains that of the final users. Yet once the decision to opt in has been made, in neither case can users control how their data and resources are used by third parties because the automated systems that manage the sharing are complex and opaque.

radio-frequency identification) along with expert systems able to merge and manage the data resulting from these systems.

Yet the increased use of electronic chips in all kinds of devices, the expansion of network uses into all domains of life, and the generalization of the ability of information processing devices to communicate—in short, the pervasiveness of computing—inevitably leads to the systematic tracking of individuals in most aspects of their life. For this reason, questions about the status of personal data have become more central. We can identify two opposed visions on this score. The first is that personal data (and privacy in general) should simply be considered as a *property* right. Thus individuals are free to transfer pieces of their private information in exchange for various benefits. This vision is promoted by those interests that believe private information is the fuel of future information services in particular and, more generally, of a society featuring highly customized services. The second viewpoint is that privacy should be considered as a *fundamental* right because it is the root of individual and collective protection against all forms of tyranny. In this view, the potential negative externalities of releasing information on individuals would justify strong public intervention and regulation to prevent overly customized tracking by any organization, public or private. This perspective also accounts for—and, in the absence of public oversight, calls for—activists to provide the means to circumvent tracking technologies.

One of the individual (and sometimes collective) responses to such threats to privacy consists of managing one's "identities"; here avatars are the most sophisticated way of proceeding. Pseudonyms, holding multiple cards, and devising "built" identities are all meant to subvert attempts to track, profile, and/or control. These tools enable individuals to live parallel lives in response to the standardization imposed by, and to the intrusive possibilities laid open by, modern societies. The resulting complex issue stems from the decreasing confidence that system users have in their ability to identify others accurately. In the end, you are never quite sure of whom (whether individuals or organizations) you are exchanging information with, having business with, or meeting online. Obvious issues of individual and collective security follow from this lack of confidence. In response, some organizations—in particular, governments and transnational corporations—might well develop unacceptably intrusive technologies to verify identities, which would constitute a major threat to freedom and individual security *unless* the type of "checks and balances" mechanisms operative in Western democracies for the last 150 years were guaranteed. But such a guarantee will be difficult to provide, given that most states are not democratic, that systems of an international scale are built by actors with widely differing interests and capabilities, that "solutions" can be (surreptitiously) embedded in the technology itself, and that there is a high risk of the network being captured or at least dominated by some governments and private providers of security, technology, or information services. Clearly, then, the challenge is to build governance frameworks that balance the need for security with individual freedom and rights. This is a context in which innovation (and therefore openness) is needed and where all stakeholder types should be encouraged to promote solutions whose adoption would appeal to many in the absence of collectively devised solutions.

1.4 Conclusion: The (Re)building of National and International Orders

As illustrated by the points we have made with regard to the management of access, flows, and identity, most of the stakes involved in governance of the Internet (and of the information society) cannot be disconnected from overarching questions about national and international government. Indeed, the fundamental issue is how individual and collective action can be regulated in an arena without frontiers—that is, without strong national borders but with strong interconnections among the various domains of public life and private industry that rely on the digital management of information.

The problem is that a laissez-faire approach, aside from possibly leading to discriminatory and suboptimal solutions, is also plainly unrealistic: many high-level actors can propose pragmatic solutions, which can be endorsed by many other actors (and also by individuals) because all actors have a fundamental need for (minimal) order and security. For this reason, a handful of powerful states may be able to establish minimal coalitions for proposing and imposing new institutional frameworks together with technical solutions implemented by such central players as the major domain names registries, search engines and web2.0 services providers. As pointed out in this book, the dynamics at play in the various interweaved domains are multiple and complex, and overall the game is open-ended.

The most obvious point is that many jurisdictional competences must be (re-)delimited, sometimes via creation of new jurisdictions. It is not entirely clear whether an integrated system of governance can be built or whether, in contrast, the only solution is to build a polycentric system based on mutual tolerance for heterogeneous practices (as regards filtering, network neutrality, trading, etc.). The integration option would inevitably start with the reshaping of ICANN, which would become a (quasi-) intergovernmental agency if the Governmental Advisory Committee (GAC) gradually took it over—as called for by the Group of 77. The second, polycentric option could be implemented as an evolving arrangement among some national governments (those of the G-20 or even only those of the G-8), a few major information technology players, and organizations such as ICANN that have developed their own organizational logic and capabilities and already represent some compromise within the technical community.

This latter, most probable scenario would develop in a context where some issues—namely, sovereignty, security, and conflict—are increasingly viewed as central while such values as fundamental rights, democracy, and the rule of law are viewed as unrealistic constraints in light of the pragmatic requirement to implement solutions rapidly. Also, efforts to establish international regulations arise in a context where the defense of diversity may well lead to a generalized and self-defeating relativism. In the matter of control or filtering of content, for instance, human rights are increasingly opposed to notions like sovereignty and cultural identity. After all, free speech tends to be contested by all kind of actors who are willing to claim defamation (against religions, employers, etc.). These trends are naturally of concern—especially for established democracies, since authoritarian regimes are not expected to tolerate (much less provide for) free speech. Note that, unlike the liberal states built in the 19th and 20th centuries, emerging orders are not necessarily anchored in the philosophy of the Enlightenment.

One force behind the evolution of the Internet Governance is the debate's enlargement beyond technical management of the network to include institutionalization of the information society. The resulting scope, technicality, and complexity of the debate means that only a small number of actors are able to manage it even as the number of stakeholders has progressively increased. As a consequence, the essential debates tend to be "captured" by a few, and minimal coalitions are able to make and implement far-reaching decisions. Reorganizing the debate is thus probably the best way to send the process of building Internet Governance down a promising path. In particular, the appropriate level of governance (together with related issues) should be determined more precisely so that an improved federal system can be built on the basis of having identified those governance levels, the principles of subsidiarity, and the interdependencies among issues. A precise mapping of the scope of alternative public goods and the most appropriate way to provide them—the issue of *aggregation technologies*[18]—would make it easier to establish not only the roles of communities, governments, independent agencies, international organizations, and so forth but also the best way to coordinate them. It would certainly be a major contribution if the academic community could pin down what is known about these issues. This contribution is necessary if we are to organize a more consistent system of authorities within a network that enables evolution *and* checks and balances, two aspects that are much needed in any context of sustained learning and innovation.

[18] This refers to how individual contributions to the collective good determine the quality of the good available for consumption (Hirschleifer 1983; Cornes and Sandler 1984). For summation goods, each unit contributed to the public good adds an identical and cumulative amount to the overall level of the good available for consumption. For example, any reduction in the emission of greenhouse gases corresponds to the aggregate (summed) cutbacks of the polluter countries. Other important types of aggregation technologies are: weakest-link public goods, where the smallest contribution fixes the quantity of the public good for the entire group (for example, pest diffusion); best-shot public goods for which the overall level of the public good equals the largest single individual provision level (e.g. finding a cure for a disease); and weighted-sum public goods where different contributions can have different impacts (as in the cleanup of polluted sites)