Francesco Amoretti. Associate Professor of Political Science and of E-democracy and E-Government Policies at the Università degli Studi di Salerno, Dipartimento di Scienze politiche, sociali e della comunicazione. His recent research activity, basically developed within the general field of relationship between media and political systems, regarded three areas which can be described as: Mediatization of politics in Italy; the electronic government, and the digital revolution and the processes of constitutionalisation.
Contact: amoretti@unisa.it

Mauro Santaniello. Researcher at the Dipartimento di Scienze politiche, sociali e della comunicazione of the Università degli Studi di Salerno. His research focuses on Internet regulation and on the relationship between digital networks and power.
Contact: msantaniello@unisa.it

BETWEEN REASON OF STATE AND REASON OF MARKET:

The developments of internet governance in historical perspective

DOI: 1017450/160109

Francesco Amoretti and Mauro Santaniello
Università degli Studi di Salerno

Reception date 8th November 2015; acceptance date 20th February 2016 this article is developed within a project research held at the Dipartimento di Scienze Politiche, Sociali e della Comunicazione, Università degli Studi di Salerno.

Abstract

"No sovereignty, no elected government, no authority, no borders". It was exactly twenty years ago, John Perry Barlow proclaimed his *Declaration of the Independence of Cyberspace*. And those were his keywords. Today, we can say that the development of Internet governance as a global policy arena is the answer to the questions that Barlow believed irrelevant to the proper development of cyberspace. If founding myths about an ungovernable, borderless, and intangible Internet have been demolished, what power relations have emerged in the Internet governance arena? What are the ideas –or the *normative values*– that sustain and legitimize the political role of governmental and nongovernmental actors? And, finally, is the *multi-stakeholder* model capable of grasping the *real* conflicts over political power, or is it part of those conflicts, a narrative supporting specific interests and coalitions? The main aim of this article is to consider these issues by analysing the developments of political conflicts over Internet governance, from the IAHC to WSIS, until recent processes such as the WCIT and NetMundial.

Key words

States, sovereignty, political conflicts, giant corporations, Internet governance

Resumen

"Ninguna soberanía, ningún gobierno electivo, ninguna autoridad, ningún confín". Hace veinte años, John Perry Barlow proclamó su Declaración de Independencia del Ciberespacio. Y estas eran las palabras clave. Hoy día, podemos afirmar que el desarrollo del *Internet Governance* como ámbito de *policy* global responde a las preguntas que Barlow consideraba irrelevantes precisamente por lo que al desarrollo del ciberespacio se refería. Una vez que los mitos fundadores de un Internet sin confines, inmaterial y falto de estructuras de gobierno han sido derrotados, ¿cuáles son las relaciones de poder que han emergido en el campo del dominio del Internet? ¿Cuáles son las ideas –o los *valores normativos*– que sostienen y legitiman el papel político de los actores gubernamentales y no gubernamentales? Además, ¿el modelo *multi-stakeholder* sabe distinguir los conflictos de poder *reales*, o él mismo parte de esos conflictos, como un discurso de apoyo de los intereses y de las coaliciones en juego? El objetivo principal del artículo es analizar esos cuestionamientos a través del análisis del desarrollo de los conflictos políticos respecto de la gobernanza de la red: del IAHC al WSIS, hasta llegar a los procesos más recientes, como el WCIT y el NetMundial.

Palabras clave

Estados, soberanía, conflictos políticos, *Giant Corporation, Internet governance*

1. Introduction

"No sovereignty, no elected government, no authority, no borders". It was exactly twenty years ago, John Perry Barlow proclaimed his Declaration of the Independence of Cyberspace[1]. And those were his keywords. These were the words –and predictions– of a visionary. It was instead the dominant conception, in those years, in the international scientific community as well as in the areas most directly involved in the design of

1. J. P. Barlow, *A Declaration of the Independence of Cyberspace*, 1996, https://projects.eff.org/~barlow/Declaration-Final.html

cyberspace. In a 1998 article by Carey entitled "Internet and the end of the national communication system" were established the general coordinates within the theoretical and empirical research on the relationship between digital media and states might be placed[2]. The diffusion of networks was redefining roles, functions, and policies of the state –of the states– involving, all in all, a negative balance for the state –less sovereignty, less authority, less regulatory capacity–, and control of information flows. In the map of the world telecommunications market, states were destined to play secondary roles; in the Old as the New continent were being celebrated the glories of neoliberal globalization. The withdrawal of states was also deemed necessary to the full deployment of the network's potential. Those who had at heart the renewal of politics; saw in the opportunities offered by digital networks a historic opportunity, one to be seized without too many ifs and buts.

With governments to act as guarantors, with specific policies, of technological innovation; keeping away the states from these processes was therefore not only desirable, but also possible, considering which way the wind had been blowing for about two decades. That it was Bill Gates to announce, in a famous 1996 speech, with the expansion of cyberspace and the creation of Adam Smith's dream of a free international market, it is not surprising. The cyber-optimists' community did not only include entrepreneurs and professionals of the computer industry. Besides these, intellectuals, professionals, politicians, and citizens looked to cyberspace as a new frontier –along the "Information Superhighway"– the old myths of American culture were being revived[3]. Subtracted to the control –and the powers– of the state, the virtual space imagined and hoped for would be a transparent and ubiquitous space; and everyone might communicate freely with one another. A free world, that of cyberspace, which would guarantee freedom for everyone. Betrayed in the off line world, the First Amendment, the true lynchpin of American constitutional and legal culture, would find in the expansion of the Network a vast territory to protect but also an opportunity to regenerate itself. The state, certainly transformed, does not abandon the scene. Yet the scene occupied by the state can neither be –nor should be– that of virtual reality which, for its characteristics, can escape its intervention. It is a "borderless and timeless world"[4], and the virtual and, as such, not disciplinable/regulating the sovereign authority of states.

2. J. W. Carey, "The Internet and the End of the National Communication System: Uncertain Predictions of an Uncertain Future", in *Journalism and Mass Communication Quarterly*, 75, 1, 1998, pp. 28-34.
3. V. Mosco, *The Digital Sublime Myth, Power, and Cyberspace*, The MIT Press, Cambridge & London, 2004.
4. R. Johnson, D. G. Post, "Law and Borders: The Rise of law in Cyberspace" in *Stanford Law Review*, 48, 5, 1996, pp. 1367-1402.

Today, we can say that the development of Internet governance as a global policy arena is the answer to the questions that Barlow believed irrelevant to the proper development of cyberspace. If founding myths about an ungovernable, borderless, and intangible Internet have been demolished, what power relations have emerged in the Internet governance arena? What are the ideas –or the *normative values*– that sustain and legitimize the political role of governmental and nongovernmental actors? And, finally, is the *multi-stakeholder* model capable of grasping the *real* conflicts over political power, or is it part of those conflicts, a narrative supporting specific interests and coalitions? The main aim of this article is to consider these issues by analysing the developments of political conflicts over Internet governance, from the IAHC to WSIS, until recent processes such as the WCIT and NetMundial. The objective is to answer the following research question: are the redefinitions of powers in such a global policy field generated by the *shifting* relationship between the *Reason of State* and the *Reason of Market*? More precisely, through a reconstruction of the main conflicts that have occurred over two decades, we can indeed describe and analyse state sovereignty in some of its concrete forms and inter-institutional dynamics. A prospect that, as we shall see, will allow us to avoid dilemmas that still run through the academic debate, dilemmas that appear historically inconsistent and, therefore, theoretically and analytically unproductive: suffice it to think, in particular, of the predicament over the true or alleged return of state sovereignty, and to the question of the relationship between public authorities and economic powers that so much play in defining boundaries and content of state authority.

But let us clarify first of all what we are referring to. Although a clear definition of Internet Governance is problematic at best –Janette Hofmann speaks of it as "a policy area with ambiguous boundaries and structures […] a normative idea on the move"[5]– it refers to the configuration and the allocation in powers for determining and controlling all levels of articulation and operation of the network –infrastructures, interfaces, devices, data centres, etc–. Beyond the technical language, Internet Governance is concerned with what the network is at a given moment in history, and with what can be done on the net and through the net[6] in different contexts and at different times. Internet governance concerns a global power struggle and its outcomes, and it is founded as a research field with the idea that the Internet is governable[7]. As Mueller has put it:

5. J. Hofmann, "Internet Governance: A Regulative Idea in Flux", in R. K. J. Bandamutha (ed.), *Internet Governance: An Introduction*, Icfai University Press, 2007, p. 75.
6. We have addressed the issue of "governance through the net" in F. Amoretti and M. Santaniello, "Governing by Internet Architecture", in *Soft Power*, 1, 1, 2014, pp. 109-127.
7. A sound definition of Internet Governance is that provided by Milton Mueller: "Internet governance is the simplest,

> The question now driving discussions over Internet politics is not whether the Net can be governed, but whether there is (or there should be) something new and different about the way we do. Does a globally connected information infrastructure require –or is it already producing– new global institutions? Asking that question leads inexorably to the issue of the nation-state and to the relationship between national and global governance[8].

The state, as political scientists insist, is still the predominant supplier of effective public governance, and it is still an immensely powerful institution. But there is a strong and persistent tension between state sovereignty, which is territorially bounded, and the non-territorial space of social interaction created by networked computers. This tension places strain on the existing nation-centered institutional arrangements in communication and information policy.

2. Internet vs the Nation-State

Three assumptions about the nature of the Internet have influenced the study of political institutions in the so-called "information age". Three great images that have often been uncritically taken for granted by social and political scientists, who have built them around post-Westphalian, post-democratic, post-capitalistic, post-human theories. The first assumption relates to the immateriality of cyberspace, that is, the idea that the Internet is a virtual world completely separated from material reality. A world of bit opposed to the old world of atoms, as stated by Nicholas Negroponte[9]. A corollary of this assumption is that in a world of bit, with its completely symbolic and reproducible resources, there is no scarcity, and that the abundance of resources inevitably produces a downfall of conflicts and, finally, the end of politics. This image strongly contrasts with the empirical reality of digital networks, which work thanks to infrastructures and devices made of plastic, metal, and silicon; thanks to transoceanic cables, antennas, power stations, and heavy geostationary satellites; thanks to computer centers as large as whole cities. All of these are scarce resources whose control produces tensions and conflicts.

---

most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies". Cfr. Note 8: 9.

8. M. Mueller, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge, 2010, p. 1.

9. N. Negroponte, *Being Digital*, Alfred A. Knoff, New York City, 1995.

The second assumption relates to the borderlessness of the virtual world, that is, the idea of a deterritorializing flow of information leading to the end of geography and the death of all distances. Even this is a mystification, as demonstrated by the many cases in which authorities of individual countries have ordered an Internet shutdown, within their borders, during the political crisis. This has happened, for example, in Syria during the early stage of riots, and in Egypt during the Arab Spring. More recently, it happened in Turkey and Burkina Faso, where national authorities have been able to block access to some specific websites (Twitter, Facebook, YouTube). It routinely happens in China and authoritarian regimes.

The third assumption concerns Internet's scalability, that is, the idea of a cyberspace that, notwithstanding its growth in terms of population, geographic extension, and interactive density, remains always the same. The substantial continuity of the Internet has as a corollary the idea of its un-governability, a hypostatization of the characteristics of the early Internet, such as openness, neutrality, decentralization, horizontality, and so on. This idea also clashes with empirical reality, particularly with the evidence of many transformations undergone by Internet infrastructures, interfaces, codes and devices over time. All transformations that have heavily defaced those traits. Transformations which are more similar to disruptions than to changes.

These assumptions –immaterial and abundant resources, borderlessness, and resilient un-governability– have inspired many studies of "Internet Governance" in which states, and governments, play an increasingly marginal role to the advantage of other institutional actors[10]. Hardly surprising, it might be said, if it is true that in the last decade of the twentieth century "outsourcing sovereignty" –i.e. the transfer of public power to other hands– has expanded in many directions[11]. Certainly, the vast majority of national governments hasalmost no power on Internet standards, protocols, and critical resources, and has only an advisory role in its main institutions, such as the ICANN. However, to speculate about the erosion of the international system of sovereign nation-states leads to some misunderstandings. Firstly, the overcoming of the post-Westphalian order does not mean that the nation-states system disappears. The emergent conditions do not *necessarily* override the sovereignty of states. Not all states are incapable of exercising control over critical Internet resources. It is not necessary to accept the *hegemonic*

10. In some cases, such assumptions have strengthened the idea of the end of the nation-state, of a decline of its functions and structures – with no spaces and physical events left on which it might exercise the monopoly of the use of force, without geographies and jurisdictions, the state would lose its own raison *d'être*.
11. P. R. Verkuil, *Outsourcing Sovereignty. Why Privatization of Government Functions Threatens Democracy And What Can Do About It*, Cambridge University Press, Cambridge, 2007.

paradigm to recognize the predominant role of the U.S. government in building and developing the cyberspace, and its effort to legitimate, also from a cultural/normative point of view, the political strategies pursued[12]. We are going to argue, in this article, that the *asymmetry* between the United States and most other countries is at the origin of *every* relevant political conflict that has shaped the Internet governance. In other words, the role of the state has always been at the core of the debate on how to govern the cyberspace, as the main controversy crossing discussions about Internet ontology and deontology. Secondly, as we shall see, the movement towards digitally bordered "national internets" or more correctly, the claim for new governmental and intergovernmental mechanisms to strengthen states over the Internet, is not taken into account by the dominant analytic perspectives. Yet, this is perhaps, in the international arena, the main political development of the last decade. Last but not least, the power relationships between states and the forces of the market are not a zero-sum game.

In the face of the capacity of the global economic actors to impose the operational logic of the capital market as a *new normativity* of national policymaking, the states do not retreat in the same way everywhere –nor do they do so– with the same outcome. As argued by Saskia Sassen in her innovative works, sovereignty and territory remain key features of the international system, even though "to some extent national states are producing the necessary instrumentalities that enable new forms of authority", notably exercised by corporations operating transnationally[13]. Anyway, it is anachronistic to refer to sovereignty and territory as features of nation-states without considering the most complex institutional and structural rearrangement of our epoch[14] (Sassen, 2013). To understand this rearrangement, however, it is useful to grasp the *shifting* relationship between the *Reason of State* and the *Reason of Market*.

12. An analytical perspective focused on the concept of hegemonic regime is in S. Bradshaw, L. DeNardis, F. O. Hampson, E. Jardine, M. Raymond, "The Emergence of Contention in Global Internet Governance" in *Global Commission on Internet Governance paper Series* no. 17, July 2015. The authors argue: "Hegemonic transition theory can partially account for some of the contentious state behaviour marring global debates concerning Internet issues. States that are currently dominant in the Internet governance regime, such as the United States, are coming into increasingly conflict with other states that hold different ideological viewpoints and that see American dominance of the system as illegitimate or even an outright security challenge. Many developing nations that have yet to fully move online are now giving voice to the fact that they are compelled to adopt a system that is governed in a way that they did not help to directly develop. Other nations, such as Russia and China, have simply transposed tensions from other areas onto the Internet governance debate, making the issue particularly fractious. Hegemonic transition theory is less able to account for the nature of the alternatives preferred by these actors, which are shaped both by domestic values and international norms, or the processes of global rule-making by which these objectives are pursued. Again, this highlights the interactions between distinct factors that collectively account for increased global contention over Internet issues".

13. S. Sassen, *Territory, Authority, Rights. From Medieval to Global Assemblages,* Princeton University Press, Princeton and Oxford, 1996, p. 233.

14. S. Sassen, "When Territory Deborders Territoriality", in *Territory, Politics, Governance*, 1, 1, 2013, pp. 21-45.

3. Conflict #1: Towards a Corporate Coalition

The first conflict for the control of the Internet set the Clinton Administration against the community of the founding fathers[15]. One of them, Vinton Cerf, had founded the Internet Society (ISoc) in the early 1990s in order to institutionalize the deliberative practices developed during the 1970s within some informal organizations such as the Internet Engineering Task Force (IETF). Aiming at stopping the ongoing privatization of the Domain Name System (DNS), ISoc launched the International Ad Hoc Committee (IAHC) in 1996, an initiative which elaborated an institutional design for the governance of Internet domains that was clearly rooted into a model of "technical regime" (Hofmann 2005), and which excluded governments –all governments, including the US government– from critical resources management and administration. Seeking to be legitimized and looking for organizational support, ISoc involved the International Telecommunication Union (ITU), the UN agency that handles interstate relations concerning telecommunications networks such as telephone, mobile and satellite networks. In front of this initiative, the US government initially announced its intention to give up its authority over the DNS root zone, but it soon made clear that no Internet institution could be established without the US government's license: "the United States paid for the Internet", the US Internet Policy czar Ira Magaziner said[16]. Against the IAHC and the so-called MoUvement (i.e. the movement which supported the new Memorandum suggested by the Isoc) doubts about security were advanced and voice was given to those big investors who claimed a protected environment for their billion dollars' investments in e-commerce.

The ITU involvement into an organization based in Geneva was condemned as the prelude of an Internet "over-regulation", as a breach through which governments could enter the operational management of the Net, and as a deadly embrace with the corrupt and inefficient world of the United Nations[17]. On January 28th of 1998, the US government definitively took away any hope from the MoUvement stating, with a Green Paper of the National Telecommunications & Information Administration (NTIA), that the root zone management would be entrusted to a private organization based in Califor-

15. The reconstruction of Internet governance conflicts presented here is a summarized and upgraded version of that presented in: M. Santaniello, "Net democracy: la sfida democratica all'Internet governance", in E. De Blasio and M. Sorice (eds.), *Innovazione democratica. Un'introduzione*, LUISS University Press, Rome, 2016, pp. 63-86.
16. Cit. in J. Goldsmith and T. Wu, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford University Press, Oxford, 2006, p. 41.
17. W. Drake, *Reframing Internet Governance Discourse: Fifteen Baseline Propositions*. Memo #2 for the Social Science Research Council's Research Network on IT and Governance, 2004.

nia. For this purpose, on September 18th the Internet Corporation for Assigned Names and Numbers (ICANN) was founded with a governance structure very similar to that designed by the IAHC, but set up as a nonprofit corporation with offices in Playa Vista, Los Angeles. Vint Cerf became chairman of the ICANN, and the "self-governance" principle, as well as the anti-government rhetoric, once banners of the technical community in its battle against the US government, became flags of the new giant corporation. And no matter if ICANN came to be formally linked, through a series of contractual obligations, to the US Department of Commerce. The outcome of this first conflict for Internet governance was the skidding of the self of "self-governance", the slipping of the subject who should govern himself: from the technical community of the founding fathers to the US private sector. It was the formalization of a process of Internet privatization that had already started in the second half of 1980s with the splitting of Arpanet into Milnet (for military purposes) and Internet (with commercial aims), and with the switching off of the early network a few months after the fall of the Berlín Wall. A process proudly defended by the US government that was able to impose the *reason of the market* over the technical community.

In that context, *Reason of the Market* means that it was the private sector in the core economies and, here, specifically transnational corporations, technology companies, large providers of digital content and information services –that took the lead in shaping the regulations thanks to and sustained by governmental policies[18]–. More specifically, according to Saleh, "when the gates of the Internet were opened to the non-academic public, including commercial users of the network"[19], core governments and ICTs companies worked out the rules that would govern online communication, consolidating a *Corporate Coalition* that acted fast as a global phenomenon on the Internet's regulatory scene. The absence of preexisting rules that established rights, duties, and entitlements in the cyberspace gave them competitive advantages in the promotion of their preferred framework of rules. Within the United States, the Federal Communications Commission treated the Internet as an unregulated application. The view was that "limited government intervention is a major reason why the Internet has grown so rapidly in the US. The federal government's efforts to avoid burdening the Internet with regulation should be looked upon as a major success and should be continued"[20].

18. These private actors dominated the development of the three main aspects of the Internet regulatory framework: (1) technical standards surrounding the Internet; (2) strategic vision for the Internet; and (3) governing domain names.
19. N. Saleh, *Third World Citizens and the Information Technology Revolution*, New York, Palgrave MacMillan, 2010, p. 57.
20. Cit. in W. J. Drake et. al., "Internet Fragmentation: An Overview", in *Future of the Internet Initiative White Paper*, World Economic Forum, 2016, p. 31.

4. Conflict #2: the dawn of multi-stakeholderism

The foreclosure to ITU meant the refusal to equate the Internet to other international networks, such as telephone and railway networks. It was supported by the affirmation of an ontological incompatibility between the Internet and the Westphalian system of interstate governance based on the borders, national sovereignty, and legal equality between states. It was backed, in other words, by the idea of "Cyberspace", a completely different social space. This is what triggered the second conflict over Internet governance. The setting was that of the World Summit on Information Society (WSIS) organized by the ITU under a mandate by the UN between 2003 and 2005. Milton Mueller, one of the most attentive observer of this process, has described it as:

> A clash between two models of global governance: one based on agreements among sovereign, territorial states; the other based on private contracting among transnational nonstate actors, but relying in some respects on the global hegemony of a single state[21].

Those described by Mueller as sovereigntists, or realists (i.e. governments other than the US one that would not tolerate the subtraction of the Internet to intergovernmental regulation) managed to impose the issue of ICANN governance on the Summit agenda in 2003, winning the attempts of the US government and ICANN itself to exclude from negotiations and final declarations any reference to domain names and Internet addresses. The Geneva Summit (2003) issued a Declarations of Principles that, at the articles concerning Internet Governance (from 48 to 50) was heavily inspired by positions –above all European and South American– that contrasted the American one. In particular, the right of governments and of intergovernmental organizations to be involved in Internet governance was clearly affirmed. On the contrary, the US government did not go beyond the assignment of advisory functions to governments within ICANN, through the Government Advisory Committee (GAC), and a promise of a complete transition, which would end the US supervision over ICANN before 2006[22]. At this point, aiming at solving the conflict by producing new ideas, the UN General Secretary established the Working Group on the Internet Governance (WGIG). WGIG's

21. Supra, note 8, p. 55.
22. This approach was expressed in the new Memorandum of Understanding between the US government and the ICANN in 2002, envisaging the end of US government supervision.

composition and its working procedures became the example of that inclusive model of Internet governance initially supported by the EU and based on the participation of multiple stakeholders[23]. Also the definition of Internet governance proposed by the WGIG was a tribute to the multi-stakeholder model:

> 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[24].

However, no US representative joined the WGIG, indicating that the US Government did not intend to grant anything to the multi-stakeholder model in Internet governance. The WGIG ended its report on June 20, 2005. Ten days later, the Bush administration issued its "US Principles on Internet Domain Name", which affirmed the exclusive and indefinitely policy authority of the United States over the Internet, and dismissed any kind of legitimacy by the UN[25]. The EU has kept advancing "a new model of cooperation" involving all stakeholders and protecting "the architectural principles of the Internet, and claiming the priority of: "the question of internationalising the management of the Internet's core resources, namely, the domain name system, IP addresses and the root server system, appears to be one of the main issues currently being discussed"[26]. Even if the European proposal suggested to focus governments' initiative on "principle issues of public policy, and [to] exclude any involvement in the day-to-day operations"[27], it was rejected by the US government with a letter sent by Carlos Gutierrez (US Secretary of Commerce) and Condoleeza Rice (Secretary of State) to Jack Straw, at the time Ministry of Foreign Affairs during the UK presidency of the EU.

23. The term "multi-stakeholder" was used within the UN, from the early 2000s, to describe a series of "civic control" initiatives in which intergovernmental organizations and non-governmental organizations "encourage companies to participate in programs that set social and environmental standards, they monitor the compliance, report and promote social and environmental auditing, certify good practices, and encourage dialogue among stakeholders and social learning" (P. Utting, "Regulating Business Via Multistakeholder Initiatives: A Preliminary Assessment", paper prepared for the UNRISD project on Business Responsibility for Sustainable Development, http://www.unrisd.org/80256B3C005BCCF9/%20(httpAuxPages)/35F2BD0379CB6647C1256CE6002B70AA/$file/uttngls.pdf, 2001, p. 2).
24. WGIG, *Report of the Working Group on Internet Governance*. Château de Bossey, http://www.wgig.org/WGIG-Report.html, 2005.
25. NTIA, U.S. *Principles on the Internet's Domain Name and Addressing System*, https://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system, 2005.
26. European Commission, *Towards A Global Partnership In The Information Society: The Contribution of the European Union to the Second Phase of the World Summit on the Information Society (WSIS)*, COM (2005) 234 final.
27. Ibid.

> As we approach the World Summit on the Information Society (WSIS), we should underscore the vast potential of the Internet for global economic expansion, poverty alleviation, and for improving health, education and other public services, particularly in the developing world where Internet access remain unacceptably low. The Internet will reach its full potential as a medium and facilitator for global economic expansion and development in an environment free from burdensome intergovernmental oversight and control. […] Burdensome, bureaucratic oversight is out of place in an Internet structure that has worked so well for many around the globe. We regret the recent positions on Internet governance (i.e., the "new cooperation model") offered by the European Union, the Presidency of which is currently held by the United Kingdom, seems to propose just that - a new structure of intergovernmental control over the Internet.[28]

Just a few days before the Tunis Summit, the US Congress unanimously expressed unconditional support to the US Principles, backed up by domestic public opinion, which mobilized against the danger of a "UN takeover". The Tunis Agenda was a mediation between these positions. WGIG's Internet governance definition as a multi-stakeholder process was kept, and a procedure started in order to establish an ad hoc forum for policy dialogue, the Internet Governance Forum (IGF), which became an annual event and a champion of the multi-stakeholder model in Internet Governance. On the other side, every hypothesis to internationalize a multi-stakeholder mechanism for ICANN's political supervision was rejected[29]. Once defeated the multi-stakeholder model as an institutional alternative to the US supervision on critical resources, the US government turned into the most active supporter of the multi-stakeholderism, but limiting it to non-binding policy arenas, like the IGF, or implementing a weak version of it where there was a real exercise of public power, like in the ICANN. Multi-stakeholderism entered ICANN's language and its official documents, just like, some years before, the self-governance flag had been lifted by the corporation after the victory of the US government over the technical community that aimed at attaining self-governance.

28. The text of the letter is available at: http://www.theregister.co.uk/2005/12/02/rice_eu_letter.
29. The WGIG had proposed four alternative models for the management of domain names and IP addresses.

5. Conflict #3: the sunset of the multi-stakeholder model

Discontent about the efficacy of the IGF in implementing the Geneva Principles arose in 2010, when China and the Non-Aligned Movement threatened to oppose the renewal of the IGF mandate for other five years[30]. Mueller[31] has described this conflict as the struggle between hawks (asking for binding declarations and effective policy-making) and doves (mainly the US government, backed this time by the EU, who understood the IGF as a non-binding policy dialogue). The IGF mandate was renewed and the doves' approach prevailed for the years to come, but, at the end of 2012, the issue was revived at the World Conference on International Communications (WCIT), held by the ITU in Dubai in order to update the 1998 International Telecommunication Regulations. These new treaties affirmed that:

> All governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized[32].

The ITU's role as a deliberative arena for Internet governance was relaunched. States were put in charge of "ensuring the strength and the security of international telecommunication networks", of preventing spam, and minimizing its impact on services (Art. 5a), enabling in this way the regulation of data flows by governments. Article 7 even disciplined the right of Member States to "suspend international telecommunication services, partially or completely". US reaction was soon to come: "the US voiced concerns that the revised ITRs aim to replace the multi-stakeholder model of Internet governance and pose threats to an open Internet. A broad coalition of non-state actors, including civil society organizations and large Internet companies, mobilized against WCIT-12"[33].

30. E. Brousseau, M. Marzouki (2015) "Internet governance: old issues, new framings, uncertain implications", in E. Brousseau, M. Marzouki, C. Méadel (eds.) *Governance, Regulations and Powers on the Internet*. Cambridge University Press, Cambridge, p. 380.
31. Supra, note 8.
32. ITU, *Final Acts of the World Conference on International Telecommunications* (WCIT-12) http://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf, 2012, p.20.
33. J. M. Chenou and R. Radu, "Global Internet Policy: a Fifteen-Year Long Debate", in J.-M. Chenou and R. Radu (eds.), *The Evolution of Global internet Governance. Principles and Policies in the Making*, Springer, Berlín, 2014, p.13.

On December 5th of 2012, while WCIT was in progress, the US Congress approved a resolution stating that:

> Whereas proposals have been put forward for consideration at the 2012 World Conference on International Telecommunications that would fundamentally alter the governance and operation of the Internet […] Secretary of State, in consultation with the Secretary of Commerce, should continue working to implement the position of the United States on Internet governance that clearly articulates the consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multi-stakeholder model that governs the Internet today[34].

The WCIT declaration, in calling for more power for governments and ITU, also appealed to a "multi-stakeholder model of Internet", but the outcome of the Conference made it clear that the US model of Internet governance had no consensus at the international level. The final declaration was signed by a majority of 89 states, against 55 unfavorable votes, and new ITRs went into effect on January 1st of 2015. After five months, in May, a similar struggle livened up the World Telecommunication/ICT Policy Forum (WTPF) organized by the ITU in Geneva.

6. Conflict #4: Unveiling the Surveillance Coalition

The fourth conflict was triggered on June 2013. Internet governance suddenly came at the centre of international tensions and public debate in every country of the world. *The Guardian,* soon followed by other newspapers worldwide, started publishing documents provided by a mole in the National Security Agency (NSA), an agency of the US government responsible for the collection, monitoring, and processing of information for foreign intelligence and counterintelligence purposes. Edward Snowden, who worked as a system administrator for a contractor of the NSA, demonstrated with its revelations that the agency had exceeded its statutory goals, creating programmes for collecting whatever data was available in the Internet, wherever it was: passing through

34. One Hundred and Twelfth Congress of the United States of America, *S.Con.Res.50 - A concurrent resolution expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived*, Washington, https://www.congress.gov/bill/112th-congress/senate-concurrent-resolution/50, 2012.

oceanic fibre optic cables, or on the American backbone, housed in the large Web 2.0 database, in the Cloud, or on social networks, or stored on the computer of any individual user. Snowden leaks showed that, while governments were being invited to discuss within multi-stakeholder forums in order to "build an information society that were popular, inclusive, and oriented towards development", the US government and its closest allies were using the Internet to set up the largest and the widest mass surveillance system ever created in human history. Snowden's revelations shed light on a type of governmental activity completely different from those debated at the WSIS, the WCIT, and the IGF, and one built on very different power relations between stakeholders.

Alongside the escalation of existing geopolitical tensions caused by this information, the scandal opened a second front for the US government. If American civil society, as well as Europe and other Western countries, had compacted around the US administration to curb the action of authoritarian countries like Russia and China, the revelations about mass surveillance rekindled the reasons for the challenge to a private regime of governance dominated by a single country. The systematic violation of civil and political rights inside and outside the United States opened a rift between the US-led multi-stakeholder model and the human rights discourse, around which movements, associations and dynamic coalitions had taken a positive dialogue with the Internet technical community. On October 7, 2013, the leaders of the organizations involved in the technical management of the network (ICANN, IETF, IAB, WWWC, Internet Society, and the five regional registry of Africa, America, Asia-Pacific, Latin America and Europe) subscribed to the "Montevideo Statement on the Future of Internet Cooperation". The statement denounced the damage done to the trust of Internet users by pervasive surveillance and monitoring activities, stated the need to evolve the multi-stakeholder model, and called for an acceleration of the ICANN's "globalization towards an environment in which all stakeholders, including all governments participate as equals"[35].

The US government reacted to the scandal of NSA-leaks by applying the same pattern it had followed in previous crises. On March 14, 2014, the NTIA announced once again the intention of the US government to initiate a transition of supervisory functions of the "root zone"[36]. The ICANN was entrusted with the task to "gather the stakeholders in the global Internet community to build an appropriate transition plan" in

35. AA.VV., *Montevideo Statement on the Future of Internet Cooperation,* https://www.icann.org/news/announcement-2013-10-07-en, 2013.
36. NTIA, *NTIA Announces Intent to Transition Key Internet Domain Name Functions,* http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-keyinternet- domain-name-functions, 2014.

view of the expiration of the IANA[37] contract on September 30, 2015. Five weeks later, the ICANN supported the Brazilian government in the organization of a multi-stakeholder meeting, NetMundial, held in Brazil on 23th and 24th of April, during which the Brazilian President Dilma Rousseff, herself a victim of illegal wiretapping by the NSA, signed the "Marco Civil do Internet", a Brazilian law to protect the rights of network users[38]. NetMundial produced a non-binding declaration that was the result of a compromise between the primeval, radical intentions of the Brazilian government, the positions of the US government, and the leadership of ICANN. The final declaration proposed a mild condemnation of mass surveillance programs, it required compliance with international human rights and called on the international dialogue in forums such as the Council for Human Rights and the Internet Governance Forum. On November 6, ICANN, together with the World Economic Forum (WEF) and the Brazilian government agency that deals with the regulation of the Internet (Comite Gestor Internet no Brasil), launched the NetMundial Initiative (NMI).

NMI established a Coordination Council with twenty four members from five stakeholder groups: technical and academic communities, civil society, governments, private sector, and organizers (WEF, the Brazilian government and ICANN). There were not representatives of intergovernmental organizations. The UN and the ITU were cut off by the Council. Some civil society organizations and some groups of the technical community, such as Just Net Coalition and the Internet Society, disassociated themselves from the initiative, criticizing the NMI because:

> Involvement of the World Economic Forum in the initiative signals an attempt by economic and political elites to secure a central role in Internet governance; that the Initiative has been organised in a top-down manner that privileges its three promoters above other stakeholders; and that devoting time and resources to the Initiative may detract from other processes such as the Internet Governance Forum.[39]

37. The acronym IANA stands for Internet Assigned Numbers Authority, and it refers to the function of DNS root servers' management.
38. M. Mueller, *The Core Internet Institutions Abandon The Us Government,* IGP, http://www.internetgovernance.org/2013/10/11/the-core-internet-institutions-abandonthe- us-government/, 2013.
39. Cit. in V. Paque, *Civil Society Coordination Group and NETmundial Initiative Information,* Diplo Foundation, http://www.diplointernetgovernance.org/profiles/blogs/civilsociety- coordination-group-and-netmundial-initiative-inform, 2014.

Moreover, the Multi-stakeholder Advisory Group (MAG) of the IGF was initially filled with "insiders of the ICANN regime"[40]. Among the 24 members of the NMI Council, nine were members of the corporation[41]. Thus, just like it had happened with terms like "self-governance" and "multi-stakeholder", the US government seized the NetMundial initiative, which was born to protect human rights and as a response to mass surveillance programs, changing its meanings and direction. At this point, the typical pattern of action of the conservative forces of Internet governance can be retraced: to announce some concessions, to hijack dissent "into harmless activities such as discussions in gigantic workshops that lack any real power"[42] as the IGF and the WSIS, ensure nonetheless significant vantage points in their agenda setting and seizing the vocabulary and narratives of the opponents. The long-term vision, however, remains the same, defended and repeated by the announcement of the NTIA:

> Transitioning NTIA out of its role marks the final phase of the privatization of the DNS as outlined by the U.S. Government in 1997. […] NTIA will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution[43].

On March 11, 2016, the ICANN finalized its proposal to the NTIA which, consistently with the NTIA conditions, excluded governments and intergovernmental organizations from the governance of Internet critical resources.

7. Conflict #5: Towards the Sharing Surveillance

Meanwhile, terror attacks in Ottawa (October 24th, 2014), in Paris (January 7th and November 13th of 2015) and in Brussels (March 22nd, 2016) had the perverse effect of limiting criticism to mass surveillance programs and to push several Western governments towards adopting for –or legalizing– policies and practices of electronic control. Just to offer a few examples, in the aftermath of the Charlie Hebdo shooting, the French Interior Minister Bernard Cazeneuve flew to the Silicon Valley to gain advice about

40. Supra, note 8, p. 116.
41. The list of Council members is available at: https://www.netmundial.org/council.
42. J. A. Lewis, "Internet Governance: Inevitable Transitions", in M. Raymond and G. Smith (eds.), *Organized Chaos. Reimagining the Internet,* Centre for International Governance Innovation, Waterloo, 2014, p. 124.
43. Supra, note 35.

surveillance by Google, Facebook, and Twitter, pointing out that "in the course of the investigation we do not want to go through the usual governmental channels, which can take a long time". In February, the Italian government adopted "urgent measures to contrast terrorism" which extended police powers in data processing, and the Italian Interior Minister Angelino Alfano met in Rome "the Italian representatives of the main web and computer giants (Google, Facebook, Twitter, Microsoft, Hp, Ibm) in order to fight terrorism". In the following months, many Western countries took measures that restricted the freedom of expression and the right to privacy, and widened the margins of manoeuvre of security agencies. Internet companies have come to be legitimized, de facto, also in Europe, in a new role as national security advisors and providers of surveillance services. However, a new conflict over Internet governance triggered soon, this time between some governments (particularly the Anglo-Saxon ones) and Internet companies. The controversy arose around encryption services offered by some Internet companies such as Facebook (for its application WhatsApp) and Apple (for its smartphones).

Encryption is a technical process of encoding information in order to avoid that unauthorized third parties can read intercepted messages between the legitimate sender and addressee. Encryption, in the Internet, has been used in military contexts and governmental environments for a long time as an essential tool to protect state secrets and communications. Its use has become more widespread, and more problematic, after Snowden's revelations about mass surveillance programmes as the public awareness about systemic threats to privacy in the Internet had the effect to raise the demand for data protection even among civil Internet users. This emerging market orientation led to a substantial change in IT corporation policies about users' data. Afraid of their loss of reputation and trust for their involvement into US mass surveillance programmes, and fearing the rise of new competitors offering alternative solutions focused on privacy, information leading companies started to offer encryption facilities through their own services. Already a few days after Charlie Hebdo shooting, the British Prime Minister Cameron expressed a strong stand against encryption and announced laws requiring of smartphones' manufacturers and apps' developers to include "back doors" into their own products enabling the access to data by public authorities. The director of MI5 Andrew Parker, the director of GCHQ Robert Hannigan, and FBI Director James Comey publicly supported him. Currently, the Investigatory Powers Bill (IP Bill), which limits encryption and extends powers for UK intelligence agencies and law enforcement for data interception and collection, is undergoing legislative scrutiny by the UK Par-

liament. In the U.S., a similar conflict arose between FBI and Apple. On February 9th of 2016, the FBI announced that it had recovered an Apple iPhone which was used by one of the shooters involved in the December 2015 San Bernardino terror attack, but it was unable to unlock the device due to the encryption of user data. The FBI asked Apple to create a new version of the phone's operating system that could be installed in the phone in order to disable encryption. Apple refused to comply, and the FBI achieved a court order, which mandated Apple to provide the requested software. Apple opposed the order, and explained its reasons in a letter to its customers, stating that the order was to create a dangerous legal precedent undermining the security of electronic devices. On March 28th, the FBI announced it had unlocked the iPhone by purchasing a tool by some professional hackers paying more than US $1.3 million. However, on April 13th, the US Senate Intelligence Committee released draft legislation that would authorize state and federal judges to order any Internet company and hardware manufacturer to provide assistance in unlocking encrypted data and to ensure they comply with such kind of orders.

This conflict, more than the others, seems to set one against the other Reason of State (particularly national security needs) and the Reason of Market (the need of Internet companies to compete in a market where privacy and data protection have become added values). However, at a closer look, governments' requests of back doors are not so disruptive for the private sector. In fact, if this kind of demands are not extemporaneous, like in the case of FBI–Apple encryption dispute, but are codified into general laws, like in the UK IP Bill and the US Senate Encryption Bill cases, there would be no competitor able to provide privacy-enabling technologies and services. Thus, these kind of *erga omnes* obligations would not damage dominant shareholders, keeping their competitive advantage untouched. The one opposing governments and Internet corporations seems like a conflict between different narratives –the governments' one about national security, and the companies' referring to the free flow of information and to freedom of communication– rather than to a conflict of sovereignty. These narratives have been often colliding, as we have seen before. But a substratum of tacit, substantial cooperation has always prevailed. It is even more probable today, when the business of Internet companies such as Google, Facebook, Apple, Amazon is itself fundamentally based on the surveillance of their customers and of Internet users[44].

44. Profiling and tracking users, collecting data about their behavior, both online (with clickstream analysis, network analysis, sentiment analysis, and other techniques) and offline (with geolocation, biometrics, sensors and robots) are practices that are commonly used in order to provide services and sell products.

8. Conclusions

Analysing the different conflicts that have emerged since the advent of the Internet as a global phenomenon through the lenses of the shifting boundaries between *Reason of State* and the *Reason of Market* has allowed us to shed light on some inter-institutional dynamics and political issues often neglected by researchers. While recognizing that such conflicts on –and around– Internet governance are the new spaces where political and economic power is unfolding in the twenty-first century, they assert that the diffuse nature of the Internet puts pressure on the traditional nation-state, increasingly attributing the control over these public interest areas to a transnational private ordering regime and new global institutions. According to this scholarship, governments continue to oversee many Internet governance functions, developing national or regional statutes related to information policy; but the overriding of the nation-state's borders in this policy domain is a crucial indicator of the weakening of state authority in his capacity to exert its power[45]. As we have said above, this is *partially* true. There is no doubt that the Westphalian order is dead, and that the dilution of the state's formal power is a long-standing trend.

Our hypothesis is that the *unequal* distribution of power within the interstate system, and the predominant (hegemonic) role of the United States in building the cyberspace are at the origins of the *main* changes in the nature, intensity, and institutional outcomes of the conflicts in the global Internet governance arena. Whether the political power of the U.S. government regulates the cyberspace to the detriment of the communities –technicians and academics– which claimed an open and uncontrolled Internet, or whether the conflicts between the U.S. government and the giant corporations of the ICTs on crucial policy domains –privacy vs security– are exacerbated; or whether it retreats from some jurisdictional domains –IANA transition– or it seems to agree with the Internet governance model it has always opposed –multi-stakeholderism– the *rationale* is basically the same: to preserve (reassert), in a changing geopolitical environment, its dominance according to the *Reason of State* as well as the *Reason of Market*[46].

45. According to Laura DeNardis, "whereas national laws and […] international treaties have jurisdictional boundaries that complicate cross-border enforcement, the Internet's intermediating infrastructures transcend these borders and are targets of intervention for content control that is not possible through traditional governance mechanisms". L. DeNardis, *The Global War for Internet Governance*, Yale University Press, New Haven and London, 2014, p. 11.

46. The rekindled interest towards the category of sovereignty needs to be placed in a historical-political scenario radically different from the past, as has been recently pointed out, among others, by Charles Maier who, in retracing the history of the state in the last one hundred and fifty years, speaks of a Leviathan 2.0 to distinguish it, in fact, from the Leviathan 1.0, designed to solve conflicts through its absolute sovereignty. A state that has been able, therefore, to reinvent itself in

The rise of a *Corporate Coalition* was a turning point. Leading authors spoke at that time of the *death of cyberspace*[47], but it was only a predictable outcome in light of the features of the geopolitical context of the 1980s and 1990s, when the U.S. government and the ICTs corporations were re-writing the rules of the Internet: a network of networks inspired to the universalistic values of Western societies. A normative and political perspective which has persisted over two decades. This perspective is still challenged by two fronts. A sovereigntist front, whose strategic agenda is driven by a coalition of states –including Russia, China and the Arab states– which has a clear, more state-centric vision of the Internet. Against them the metaphor launched in the public debate by the Western countries is that of "balkanization", i.e. an Internet digitally divided according to national or macroregional segments. Another front is that of the constitutionalists, who would limit the power of both state and corporations by elaborating a set of binding principles framed within the international human rights law and, more recently, in national constitutions. This democratic challenge to Internet governance is supported by a heterogeneous set of actors, ranging from global civil society organizations to national parties and parliaments. The aim of this type of initiative is to produce concrete legislative outputs and further a substantial policy change.

In any case, the issue of the enforcement of those laws that protect and promote rights remains outstanding. Violations of these, in the cyberspace, can be extremely difficult to detect and prosecute. In the case of mass surveillance and censorship, the citizen is confronted by state apparatuses and giant corporations and, even when he can prove that he has suffered a violation, he is not always able to gain effective legal recognition. For these reasons, an effective democratic strategy for the Internet, beside the production of normative standards at national and international levels, needs a concrete political initiative on technical standards. As DRM technologies protect digital property rights, digital rights of the person are in need of consistent architectures and codes inserted directly into the design of media, platforms, and infrastructures. This orientation can be found in the field of protection of privacy, in some well-known design practices such as "Privacy by default" and "Privacy by Design" (PBD), and in the architectures of the so-called "Privacy Enabling Technologies" (PETs).[48]

---

many ways, coming to achieve, in this period of history, a precarious balance with economic forces that seem even more powerful than itself.

47. L. Lessig, *Code and other laws of Cyberspace*, Basic Books, New York, 1999.

48. D. Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21th Century*, Springer, Berlín, 2014.