GovReg

WORKING PAPER SERIES

Legitimacy as a Driver of the Competition between Institutions of Internet Governance

Éric Brousseau

June 2021

RESEARCH

Dauphine | PSL

CHAIRE GOUVERNANCE ET RÉGULATION

Legitimacy as a Driver of the Competition between Institutions of Internet Governance

Eric Brousseau

June 2021

Abstract:
This chapter considers the history and debates around Internet governance in an attempt to explain how multistakeholderism - embodied in the Internet Corporation for Assigned Names and Numbers (ICANN) - substituted the multilateral model of governance that prevailed in the pre-Internet era under the auspices of the International Telecommunications Union (ITU). The extent to which the outcome of the confrontation between ICANN and ITU reflects the superiority of multistakeholderism over multilateralism is discussed in detail. Both organizations' development paths and histories are assessed to understand the circumstances which led the US government to propose an alternative to an intergovernmental organization, which was then supported by a large coalition of players. The current limits of the regime that now governs the Internet is also reviewed, while its open-ended character is highlighted. Finally, an analysis is offered of the game of legitimacy establishment that has been played, and how ICANN, to date, has remained ahead.

Keywords:
Cyber-security; Digital Constitutionalism; Intergovernmental Organization; International Regime; Internet History; Multistakeholder Governance; Political Legitimacy; Standardization Process; Technical Community; Telecommunication Union;

Introduction: Competing Regimes of Transnational Governance

Under the presidency of Donald Trump, post-WWII multilateralism came under unprecedented stress. For the "hawks" in Washington, intergovernmental agreements and the related organizations were obstacles to be bypassed. These agreements were eschewed in favor of arm's-length bilateral relationships among sovereign states, under a supposedly rational divide-and-conquer strategy by the world's most powerful government, in an effort to resist coalition-building by other nation-states, and to contain challenges from rising powers and economies. Indeed, the model of transnational governance that came into being following WWII and the Cold War has been widely criticized by many stakeholders, both for its lack of effectiveness and its lack of accountability and democratic control, and seen by many as subject to obscure diplomatic bargaining.

In this context, alternative models of transnational governance have been extensively discussed, in particular "multistakeholderism".[1] This model relies on all affected stakeholders openly and directly participating in governance. Advocates highlight the effectiveness and legitimacy of such a principle. It is seen as a way to achieve democratic representation while avoiding capture by politicians and bureaucrats and shunning the electoral politics. In the realm of global governance, the roots of governance through stakeholder interaction date back to the establishment of the International Labor Organization (ILO) in 1920 and the International Organization for Standardization (ISO) in 1947. More recently, multistakeholderism has been established as the most appropriate model for governing digital resources and services. This chapter considers the history and debates around Internet governance in an attempt to explain how multistakeholderism substituted the multilateral model of governance that prevailed for telecommunication in the pre-Internet era. It goes on to question the sustainability of this model of governance and discuss its strength and benefits as well as its weaknesses and costs.

This confrontation between two models of global governance is embodied in the de facto competition between two organizations. On the one hand, the United Nations International Telecommunications Union (ITU), a classic supranational organization comprised of representatives from national governments. On the other hand, the Internet Corporation for Assigned Names and Numbers (ICANN), which groups corporations,

NGOs, experts, governments and all kinds of state and non-state actors on equal footing. As will be discussed, the former failed on several occasions to gain control of the governance of the critical Internet resources over which the latter has oversight. Although it claims to be a multistakeholder, de facto international organization, ICANN is a non-profit organization established under US law. It was set up under the leadership of the US government in the late 1990s, following which the latter progressively relinquished its control over the organization, making it progressively "accountable" to a "global multistakeholder community".

Before delving further into the history of these two organizations and the competition between them, I briefly highlight the issues at stake. Although both organizations seem to oversee obscure or secondary technical issues, the operations they manage are in fact crucial. Indeed, the services delivered over the global communication infrastructure must be translated into technical operations. The global information infrastructure, the Internet, is not a single entity, but is made up of hundreds of thousands of interconnected networks linking billions of computing devices. These networks and devices interoperate through a set of standards and protocols, and can work on a decentralized basis because they comply with a common principle of network architecture, called "end-to-end," where the network is neutrally managed in order to allow the devices to directly interact with each other. These common principles and standards provide the Internet with its features of universality, reliability, openness to innovation, and flexibility in its uses. In practice, they establish the range of possibilities in matter of security, identification, communication management impacting the way users can interact and transact on-line. In turn, any rule - either a bilateral one established by a contract, or a collective one applying to a community - has to be translated in technical operations so that it is implemented by the interconnected devices processing information. The famous adage "Code is Law," claimed by Lawrence Lessig in 1999, certainly applies here. The uses of the Internet and their regulation (either by laws or private arrangements about commerce, privacy, freedom of expression, access to information, etc.) are strongly intertwined with its technical governance.

The stakes of Internet governance are, moreover, considerable given the pervasiveness of the infostructure, which is not only global but also multi-purpose, impacting all aspects of human and societal life. The nature of the Internet - a set of shared norms and open-access resources - explains this ubiquity. Initially developed in the specific context of federally funded research, the US government made them freely accessible to industry starting in the late 1980s, and then to all potential users and developers worldwide in the 1990s.[2] By adopting these standards and principles, users have had free and easy access to a global information and knowledge infrastructure, offering exposure to a wide array

of resources, innovations, and peers. These advantages underlie the rapid and global adoption of the technology and deployment of the infostructure.[3] Not only does this resource already reach about half of humanity, but it also supports activities of all kinds. Indeed, from its origins as a communication infrastructure, the Internet has expanded into an infostructure that allows users to not only to transmit and share information, but also to deliver online and offline services and activities. In addition to the convergence between telecoms, media, and the entertainment industry, the Internet has led to a blurring of traditional boundaries across sectors, activities, communities, and even nations, as well as within the domains of individual and social life. It is then unsurprising that the prevalent governance regime for telecommunication infrastructure has not been a perfect fit for the infostructure. These elements, however, do not suffice in explaining the present governance regime organized around a non-for-profit organizations established in the US. This paper aims at critically analyzing the underlying trajectory and its drivers.

This chapter begins by describing the confrontation between the ITU and the ICANN. While the Internet is not governed by a single organization, ICANN plays a notably central role in a polycentric system. A discussion follows on the extent to which the outcome of the confrontation between ICANN and ITU reflects the superiority of multistakeholderism over multilateralism. Both organizations' development paths and histories are assessed, though one is far more recent than the other. The current limits of the regime that now governs the Internet is then reviewed, while also exploring the circumstances leading to the US government's proposal of an acceptable model of governance, which would progress in an open-ended fashion. Finally, an analysis is offered of the game of legitimacy establishment that has been played, and how ICANN, to date, has remained ahead.

1. The Internet Governance Landscape

The ITU was established in 1865,[4] making it the oldest intergovernmental organizations (IGO). Within the ITU, governments and the private sector work together to coordinate the operation of telecommunication networks and services to advance the development of communications technology. The Union consists of 193 Member States, making it one of the most inclusive IGOs, with more members than the United Nations (UN, 192). It also has over 700 Sectoral Members (commercial suppliers) and smaller associations (Partner Members), which are considered interested parties (ITU 1994a). The organization is

responsible for establishing worldwide standards that foster the seamless interconnection of a vast range of communications systems, as well as regulating and optimizing wireless communication networks and improving telecommunication infrastructure in the developing world. Interestingly, from its foundation, the ITU has not only managed technical standardization, but has also established common economic and terms-of-service principles (e.g., related to the privacy of communicated content). While non-state actors can present their views and be involved in the preparatory stage of decisions, the decision-making power remains in the hands of national governments, on the basis of one state, one vote. Government representatives gather in Plenipotentiary Conferences every four years and decide on the composition and organizational structure of the ITU, its financing, and the wording of official documents, if necessary.[5] In a nutshell, this very well-established IGO is responsible for the governance of the world's communications infrastructure, though not the Internet.

The governance of the latter seems to have fallen into the hands of a very different organization. The ICANN was created in 1998 through a Memorandum of Understanding with the US Department of Commerce. Directed by an internationally constituted Board of Directors, ICANN is a private Californian nonprofit public-benefit corporation that manages and oversees the critical technical underpinnings of the Internet: the addressing system and the communication protocols. ICANN makes its policy decisions through a multistakeholder model of governance with a bottom-up collaborative process that is open to Internet stakeholders from all constituencies. National governments gather in a dedicated working group—the Governmental Advisory Committee (GAC)—whose role is to "discuss issues with the ICANN Board and other ICANN Supporting Organizations, Advisory Committees and other groups and deliver regular advice" (cf. the website of the GAC, https://gac.icann.org/, last accessed Dec. 2020). ICANN presents itself as a forum that brings governments, users, and the "technical community"[6] together on an equal footing, promoting a multi-stakeholder approach of soft and flexible technical regulation.

At first glance, ICANN's mission is not to regulate the Internet, but rather to ensure the stable and secure management of its addressing system. As we will see in greater detail in the following section, however, this system plays a key role in ensuring access to the Internet by any user or service provider, which has made ICANN into a potential enforcer of last resort of any Internet regulation, as it can deny access for non-compliance.[7] ICANN therefore plays a crucial role in the ecosystem governing the critical resources of the Internet and, thus, the use of the latter.

Beginning in 1998, the ITU attempted to conclude an international agreement that would have seen it become responsible for regulating the Internet,[8] both at the technical and

at the use/service level. This, of course, would have required the ITU to gain oversight over the resources and functions managed by ICANN. In the context of these efforts, the ITU and the UN organized a series of two international conferences: the World Summits on the Information Society (WSIS), held in Geneva in 2003 and Tunis in 2005. The clear aim of these conferences was to discuss and establish an international convention (see, among others, Collar and Girasa, 2010; Take, 2012). The main outcome of these initiatives was the creation of the Internet Governance Forum (IGF), which has been organizing meetings since 2006 in which "people from various stakeholder groups" (i.e., not representatives of any organization) gather together to "discuss" (i.e., not negotiate) public policy issues related to the Internet.[9] At the last meeting of the WSIS, held in Geneva in 2015, the mandate of the IGF was extended to 2025, though its work has not resulted in any international agreements to date.[10]

Since the result of the WSIS process was a series of endless discussions, the ITU subsequently attempted to create a role for itself in the field of Internet regulation through another channel. In 2012, the World Conference on International Telecommunications was held in Dubai. The event was a regular ITU plenipotentiary conference organized with the aim of revising the latest version of the International Telecommunication Regulations (ITRs) adopted in 1988.[11] The clear objective of the meeting was to place digital communications within the historic mandate of the ITU, thus granting the ITU the responsibility to oversee regulations concerning network security, unsolicited communication, and, broadly speaking, Internet technical governance. Yet, the summit was failure for the ITU. While 89 states, including China, Russia, and many Arab states, voted in favor of the new treaty proposal, 55 states, including the US, the EU Member States, most other OECD Member States, and countries such as Mongolia, India and Peru, refused to sign and openly resisted the final resolution. The attempt to build a multilateral framework for Internet governance fell short, with most Western countries, backed by certain major emerging powers, defending the "multistakeholder" approach of Internet governance embodied by ICANN. The main argument in favor of the status quo was that the multistakeholder model had been able to guarantee neutrality and openness of the digital infrastructure. Meanwhile, those favoring a multilateral approach defended the idea that the principle of sovereignty should prevail on the Internet, allowing legitimate governments to oversee the management of digital infrastructure in order to regulate service provision, including the circulation of content.

In spite of the success of the US-led coalition in maintaining the status quo with respect to the role of ICANN, the US government moved towards giving up its direct control over Internet governance in 2014. Specifically, the National Telecommunications and Information Administration (NTIA) of the Department of Commerce, which held a "stewardship" role over the addressing system of the Internet,[12] announced its intention

to transfer its responsibility for the Internet Assigned Numbers Authority (IANA)[13] to the "global Internet multistakeholder community". The clear goal was to transfer it to ICANN. This transition took two years and was only achieved in October 2016. Indeed, the US Congress and several government agencies voiced doubts regarding the legitimacy, legality and risks of performing such a transfer to a non-governmental organization, even one based in the US. Within the US, those in favor of the transfer noted that much of the US jurisdictional power would remain largely unchanged, and that the transfer would strengthen the credibility of ICANN. Meanwhile, their opponents pointed out that the oversight over the addressing system is an element of sovereignty, noting that the status quo had been a strong guarantor of the openness of the Internet (a major driver of its global adoption) and a way to limit the influence of (non-US) governments that wished to take control of Internet infrastructure. The lengthy debate resulted in conditions being imposed, with ICANN required to implement reforms to satisfy four principles: the sustainability of multistakeholderism, the security, stability and resiliency of the Internet infrastructure, a high quality of service to Internet users, and protection of the openness of the Internet. This triggered anew an international and multistakeholder conversation about suitable models of Internet governance.[14] In spite of their international impact, however, these discussions did not occur in the framework of an international conference or negotiation since they concerned US legal arrangements relating to a US-based organization.

This re-organization of ICANN and of its relationship with the US Government echoed the fact that its initial design established in the late 1990s was a provisional pragmatic solution to a situation of considerable tension and confusion in the relationships between the various stakeholders of the Internet when it went commercial and international (cf. section 4). The then implemented provisional solution enabled the US government to maintain, for more than 15 years, its leadership over the governance of the Internet while also preempting the formation of any coalition strong enough to generate major changes in the status quo (as demonstrated by the Dubai failure). The revelation by Edward Snowden of the existence of the PRISM program of systematic surveillance run by the National Security Agency (NSA) undermined however the US government's claim of being a guarantor of the integrity and neutrality of the Internet as a public good accessible to all (e.g., Liu 2014; Shen 2016, Zeng et al. 2017). Support for the status quo in Internet governance weakened even among the Western allies of the US, along with a large part of the technical community; which triggered the evolution.[15]

The remaining sections of this chapter attempt to better understand how the US has ultimately been able to retain control over the design and evolution of the governance system overseeing the performance and the regulation of cyberspace, while avoiding the emergence of a multilateral system more in line with the global nature of the Internet and

its status as an essential resource. One frequently made claim is that the multistakeholder principles embodied in ICANN are both more efficient and impart greater legitimacy to govern such a technically complex global public good. Another assertion is that ICANN does not regulate the Internet, but rather contributes to its "neutral" technical governance, making US leadership of the organization a non-issue. The next section challenges this argument by highlighting the ICANN's centrality in the digital governance ecosystem, thus questioning the neutrality, effectiveness, and legitimacy of multistakeholderism in action.

2. The Centrality of ICANN in a Polycentric System

The centrality of ICANN in Internet governance is intertwined with the entrenchment of norms and governance principles in digital systems. Since the digital infrastructure comprises a wide set of technologies, supports an immense array of services, and is used by a wide variety of organizations, relational networks and service providers, a diversity of stakeholders is involved in its regulation and daily management, resulting in a distributed system of governance. In this ecosystem, however, some nodes are more central than others, and ICANN's control of the addressing system places it in crucial position.

2.1 Technologically Embedded (Self)-Governance

The Internet is based on several essential principles, which are briefly discussed here so as to elucidate the specificity of technical and non-technical governance in the field. The logic of the Internet is to interconnect information processing devices and allow interoperability between them. These devices are responsible for processing content and managing communication among themselves to ensure circulation of raw data, instructions, processing results, etc. This is referred to as the end-to-end (e2e) principle, initially formulated by Saltzer et al. (1984). It states that access and use of applications on the network should be nondiscriminatory, meaning that users on the edge of the network should freely control applications and services and be able to develop new applications. An associated principle is network neutrality, which can be defined as the "right of users to access content, services, and applications on the Internet without interference from network operators or government," and the "right of network operators to be reasonably free of liability for transmitting content and applications deemed illegal or undesirable

by third parties" (Deibert & Crete-Nishihata, 2012). Indeed, the basic principle of the Internet is that there is no distinction between the management of information flows and the processing of the circulated information. This is not the case for traditional communications networks like the telephone system, where switches are managed by network operators to interconnect equipment worked by the users. Such an organization triggers a hierarchy, whereby telecommunication operators can allocate communication capabilities, manage network access to service providers, or even control how users can interact. The logic of the Internet only allows operators to facilitate interactions among users that can fully control the circulation of information among themselves.[16]

The direct consequence of the e2e logic is that the Internet becomes a space that is open to self-governance by "users".[17] On a digital network that complies with the e2e principle, the interactions among "users" are governed by two vectors: the code and the ability to create and control information spaces. As pointed out by Lessig (1999), encoding technologies —i.e., encryption and display software—may allow the creator or owner of a digitized resource to control how it is accessed and used by third parties. This potentially permits the settlement of bilateral self-enforceable contracts, since the technology will guarantee compliance (e.g., by denying access in case of non-payment).[18] Current blockchain technologies represent, in a sense, the quintessence of this logic, since they enable to fully distribute the enforcement of contracts, or any collective rule, across computing devices. This frees such transactions from the need to rely on a third party—such as the state or an intermediary—to guarantee compliance.

The second dimension of self-regulation comes from the control of communication by users of an e2e network. Indeed, the combination of the ability to encrypt communication, control access to computing devices, and manage access to information, allows users to establish information spaces such as virtual private networks, secured websites, restricted access information sharing systems, etc. Gatekeepers to such spaces become potential rulers. Not only can they design the way users interact within the information space, but they can constrain their behaviors in the real world for fear of being denied access in the digital realm. Since the enforcement of these rules are based on the (technical) ability to include or exclude users from the information space, this is clearly a tool of self-governance by Internet users, who can then decide how these collective rules are decided and implemented, whether unilaterally or by a community. As long as the technical principle guaranteeing the e2e nature of the Internet is ensured, Internet users can thus implement self-governed orders at a low cost without needing any intervention by a supreme authority (either a government or a network operator) to guarantee these bottom-up orders. These elements are the foundation of the economic and civic dynamism of the Internet and have boosted its widespread adoption. They are

also the reason for its global nature, since governmental intervention and international agreements were not required for it to operate.[19]

However, such a decentralized system must rely on shared technical principles, and the operation of essential resources: the so-called critical resources of the Internet.[20] The e2e principle requires that devices connected to the Internet should have a single identifier (Internet Protocol (IP) addresses) and that applications running on these devices (and across multiple devices) should also have single identifiers (Domain Name System (DNS) addresses) so that the necessary dialogue between these devices and software may occur on a fully decentralized basis. In addition, these devices and software must have common languages to ensure interoperability, hence the need for common standards of communication, data management, etc. Since interoperability is not limited to the exchange of information across devices and software, a variety of standards other than the IP and DNS address systems are needed, such as the HyperText Markup Language (HTML) to display contents in web browsers. Furthermore, common principles of management must be established and complied with to ensure decentralized operation of Internet infrastructure, including principles of access and interconnection, the role of technical operators, the protection of the integrity of exchanged data, security breach management, etc. In practice, the related principles and standards are designed and administrated by a set of sui-generis organizations; often qualified as "Organically Developed Institutions" (ODIs).[21]

At this point, two observations should be made. First, digital technologies by themselves do not impose the e2e on digital networks. Indeed, a global digital infrastructure could have been developed based on administrated networks (an approach favored by the ITU and ISO; cf. note 20 and § 4.3). As highlighted by scholars such as Wu (2008), such an approach would have had the advantage of relying on negotiated transnational agreements to address the issues linked to the management of priorities, security of communication, etc. Furthermore, these agreements would have been technically implemented by network operators under the responsibility of national governments, which would have been able to formulate national-level (legal) norms using the internationally agreed transnational norms as a starting point. The e2e approach, however, had the strength of not requiring negotiation by marking available on an open access basis the core resources and standards of the Internet. Potential users simply had to adopt these standards in order to be included in the digital infrastructure and to benefit from the positive network externalities provided by other users, triggering a virtuous cycle of adoption.

The strength of this model of diffusion has been reinforced by another innovation in the realm of technical standardization: the principle of Rough Consensus, directly inherited

from the logic of software development.[22] Software is developed through the pragmatic implementation of local solutions or patches, which are tested and used until a superior patch is implemented. In the early days of Internet standardization, engineers came up with a method that was inspired by a similar logic to elaborate standards, called the Request for Comments (RFC). The later are recommendations, which are not set in stone, but rather illustrate how and why conclusions were reached, inviting interested parties to pitch in and work on the proposal, or to simply refuse them outright if a convincing enough argument could be made (Pelkey, 2007; Datysgeld, 2018). Thus, a proposal is considered to be adopted if no convincing objection is made. This pragmatism allowed a very agile adoption of a wide set of standards, including, of course, some that were developed in settings other than the original community at the origin of the Internet. This fostered the adoption of innovation (new functionalities and new languages) at a very high pace.

Second, the additional comparative advantage of the e2e model over administrated networks is that e2e allows the implementation of administrated sub-networks, while the reverse is not true. Indeed, an organization or a government can decide to implement a closed information space in which it can impose its own rules on users. The cost of such a solution, however, is that users of the closed space cannot freely interact with the other users of the Internet, resulting in losses of positive network externalities, which are higher for the users of the sub-network than for those of the generic network. Moreover, the 'ruler' of the sub-network would control the access and information flows to the gateways allowing exchange between users of the closed sub-network and users of the generic open network. This clearly presents a dilemma because flow control is costly, including in terms of time response delay and available bandwidth for users, which undermines the quality of the services that can be operated on the network. In dynamic, the creation of an alternative network is qualified as "forking"[23] since it engages the two resulting networks in different dynamics of evolutions, triggered by contrasted paths of development of software. As time goes, the applications running on the two networks, from communication management to the various application, are very likely to become increasingly incompatible. Both, static and dynamic costs, explain why even a country like China, does not establish its own Internet.

2.2 A Distributed System of Governance

The provision of a single and open addressing system along with open standards of communication is a necessary—but not sufficient—condition for the Internet to operate. In practice, compliance with shared principles and the provision of a wide set of additional services are needed to deal with issues such as cybersecurity, privacy, identity, network optimization, and the avoidance of congestion. In addition, processes and

services must be established to secure commercial and civic transactions, protect property and civic rights, settle disputes and prevent conflicts, and potentially to control content circulation. The aim of these measures is to ensure that users benefit from the possibilities of the digital architecture while also dealing with the unintended consequences of the Internet (e.g., stealing of reputation, viruses and malware, data accumulation, information manipulation). Therefore, the scope of internet governance is not a single, unitary function or practice, but rather, a complex articulation of technical standard setting, resource allocation, legal arrangements, and on-line service provision.[24] Actors are therefore numerous and diverse.[25] Moreover, a myriad of stakeholders has initiated fora, processes, and organizations proposing solutions, pushing for their adoption, expecting that positive network externalities would result into widespread adoption of their preferred norms. The bottom-up process of design and adoption of standards, combined with the scope of the stakes, combine to explain the diversity and the intensity of the involvement of stakeholders in this governance process.

Also, because of its generalized, worldwide adoption, the Internet challenges jurisdictional borders and makes it difficult to ascertain which legal norms (if any) should be considered when dealing with the framing of civic and economic activities carried out over the network. Internet activity is largely aterritorial since one of the principles of the e2e architecture is that many operations are distributed among the available resources. Thus, the legal norms to be applied are unclear and the potential conflicts of norms are numerous. Indeed, countless transactions cross international boundaries and thus blur the lines between legal operations and infringements. Moreover, jurisdictional challenges directly impact policymaking. Some aspects of governmental policies can be bypassed by Internet users (e.g., hidden commercial transactions that evade fiscal and regulatory obligations) and governmental capabilities may be compromised through the Internet (cyberattacks, intelligence). Since the Internet directly challenges sovereign states and the national social contract over which they preside, the governments call to have a greater voice in this process.

Given the multiplicity and diversity of Internet stakeholders, the variety of issues at stake, and the above-mentioned strategies to establish standards and principles to be "plugged into" the existing set of norms, several fora, organizations, and frameworks have come to occupy varying roles in Internet governance.[26] The result is "a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages" (Nye, 2014).

2.3 The Centrality of ICANN

Such a web of heterogeneous bodies with overlapping responsibilities can give the impression that Internet governance is a polycentric model without a hierarchy or central node. However, ICANN seems to be much more influential than any other body in this complex system. This is due to its central role in technological governance and its network of formal relationships with other organizations involved in Internet governance.[27]

From its creation, ICANN has been tasked with guaranteeing the end-to-end nature and the homogeneity of the Internet. ICANN's role is to ensure that each device or service provider connected to the web has an identifier that is globally unique and universally accepted. This is done by maintaining a registry of the authorized and recognized addresses and implementing policies to create new ones. Furthermore, ICANN is responsible for maintaining the registry of the instructions that are recognized by all devices and software that use the Internet Protocol to communicate. Together with Verisign, ICANN is also responsible for propagating these registries to all Internet users. This is done through a set of servers that copy the root zone of the Internet and make the information accessible to service operators and network administrators of all kinds. Not only does ICANN set the shared system of references that lies at the core of interoperability for Internet-connected devices and software, it also implements and enforces many of its policies and rules through contracts with domain registries (companies and organizations that operate and administer the master database of all domain names registered using top-level domains such as .com and .org) and accredited registrars (the hundreds of companies and organizations that consumers use to register domain names).

This position in the technical governance of the Internet makes ICANN the only central body equipped with the ability to enforce norms and with real transnational reach. Other organizations seeking to fill such a role must either deal with or be involved directly in ICANN in order to have their own norms technically recognized within the infostructure. This was the case, for example, when the World Intellectual Property Organization (WIPO) sought to make trademarks enforceable in the DNS system.[28] ICANN is thus recognized as occupying a central node in the constellation of organizations that regulate Internet affairs. These organizations, in turn, grant ICANN a clear leadership capacity and political influence as the only actor that can centrally govern issues related to the Internet. Moreover, ICANN benefits from a high level of credibility because of the technical success of the Internet. Despite continuing challenges, the fact that the Internet works consistently on a functional level is often presented as a success due to the neutrality and leadership exercised by ICANN (Take 2012; Carr 2015). Finally, thanks to the revenue

generated by selling domain names, ICANN can subsidize many organizations and initiatives related to the development of the Internet. The fact that the activities of the Internet Engineering Task Force (IETF) are sponsored by ICANN certainly contribute to the latter organization's ability to play a major role in strategic choices regarding Internet governance.

Despite its low profile in matters related to governance - ICANN always presents itself as a neutral organization in charge of the technical governance of the Internet[29] - its legitimacy has been a subject of debate, particularly due to the widening scope of the Internet. Indeed, from the latter's beginnings as a scientific network, it has grown to encompass a global economic, social, and even governmental infrastructure that has become a pervasive infostructure present across all human activities. Moreover, current trends such as the Internet of things (IoT) and artificial intelligence (AI) have increased its purview. Cerf et al. (2014) analyze ICANN's centrality in the Internet governance ecosystem, while Testart (2014) explains how ICANN has established its position. [30] Broadly, its centrality in the web of actors involved in the operation and evolution of the Internet relies on functional, contractual, and network-topographic factors that confer veto and leadership capabilities that no other body can match.[31]

3. The Competition between Two Models of Governance

According to its supporters, ICANN's contribution to the Internet governance system is a non-issue for three main reasons. First, it neutrally manages the infrastructure of the Internet, letting relevant stakeholders of all kinds implement policies and political regulations at the service level. Second, ICANN's neutrality and efficiency are guaranteed by its reliance on multistakeholderism, which ensures access of all relevant parties to the negotiation table. Third, the multistakeholder model has proven to be a superior principle of governance than its alternative: multilateralism. The following sections revisit the debate over these two models before delving deeper into the conceptual and practical limits of multistakeholderism and the specific implementation of this principle in Internet governance.

3.1 Two Opposed Models?

In addition to being software engineers and computer scientists, the Internet's initial developers were also libertarian militants who realized that the traditional system of

making and implementing policy allowed some groups to capture the collective will. Hence, the fully distributed nature of the Internet was aimed at supporting a societal governance system that relied on digital technologies to allow horizontal coordination and decision making. This vision is well-illustrated by the famous "declaration of the independence of cyberspace" by Barlow in 1996.[32] Digital technologies were understood as having the capacity to synergize disparate information streams and layers, allowing them to manage open discussions and consensus making at a large scale. Furthermore, this could be achieved without the need for a secretariat or coalitions in position to elaborate synthesis or manipulate voting processes (Aguiton and Cardon, 2012; Farina et al. 2014). In addition, the principle of rough consensus in norm making allows fixing bugs and upgrading on an ongoing basis. Multistakeholderism has been then understood as a second-best workable solution to manage the scaling-up of the Internet once it grew from a small and uniform community of users-developers to a highly heterogeneous global group of users with a variety of profiles and roles. The ecosystem built for the technical governance of the Internet has been qualified as a set of organically developed institutions (e.g., Chenou & Radu 2014; see also note 22) opposed to the political hierarchies that would be put in place by a multilateral arrangement between sovereign states.

Multistakeholderism[33] has generally been regarded as a form of participatory democracy that aims to bring together all stakeholders in a new form of communication in order to legitimize decision making at the international level (Glen 2014). By enabling non-state actors to participate in norm development and the implementation of international policies, multistakeholderism advances inclusiveness and representativeness (Jayawardane, Larik & Jackson 2015). Not only is the multistakeholder model widely regarded as the best approach to governance of the Internet, some also see it as offering a means of overhauling global governance more generally. As reported by Sholte (2017), this view comes from a recognition of the limitations of state-based democracy, particularly in the context of governments capturing the notion of collective interest in international relations, bargaining among sovereign states, and sometimes doing so in opposition to their citizens' preferences (see Herrmann-Pillath, 2022). Multistakeholderism is also understood as an alternative to build an international democratic order, surpassing the difficulties in erecting a global federalism. The model promotes an alternative to electoral politics in an effort to achieve democratic representation by including all groups that "have a stake" in the particular area or issue. It is also flexible in its implementation, which can be done through policy fora or external consultations by regulatory institutions of civil society organizations that (purportedly) represent various affected groups. Since the resulting ODIs and institutional arrangements are not grounded in formal treaties, pursuing regulatory aims through

informal memoranda of understanding rather than officially binding international law means that they can be established relatively easily and tend to be flexible and adaptable. They can also have different purposes: decision-making fora (like ICANN) are complemented by consensus-building ones (e.g., IGF). The increased effectiveness of the solutions proposed by the former approach and the democratic legitimacy of the latter one allows multistakeholderism to maximize the benefits of crowdsourcing (Nonnecke and Epstein, 2016).

Against this view, the multilateral approach views cyberspace in Hobbesian terms (Liaropoulos, 2017). Cyberspace reflects traditional power structures and mirrors security dilemmas and power antagonisms between state and non-state actors (McEvoy Manjikian, 2010). It has traditionally been supported by Russia, China, India, Iran, and Saudi Arabia. It is also popular among most developing states, which consider the present governance model of the Internet as a way for Western governments and dominant tech corporations to consolidate their domination of cyberspace and threaten national sovereignty.[34][35]

3.2 Multistakeholderism: Pros and Cons

Aside from the diplomatic debate, a large body of literature has reflected on the theoretical and practical benefits and costs of multistakeholderism. This section endeavors to synthesize this analytical discussion, while the following section highlights several essential features of the ways these principles have actually been implemented in Internet governance.

As a principle, multistakeholderism deals with the organization of an ecosystem without leadership and central place (the so-called rainforest), which guarantees the participation of all stakeholders in their respective roles on an equal footing. Furthermore, it seeks to develop policies on a bottom-up basis, using a process characterized by transparency and openness. This vision is very much in line with the Cathedral and Bazaar models proposed by Raymond (1999) to characterize alternative processes of software development. In the Cathedral model, the software code can only be viewed by a defined hierarchical group of software developers. By contrast, in the Bazaar model, code is shared openly over the Internet and with the public, subject to comment by all. The claimed advantages of the latter model lie in its ability to more effectively recognize and accommodate a multitude of interests, to optimally utilize the expertise of the crowd,[36] and to accommodate the diversity of cultural backgrounds necessary to address complex issues (which may involve political, technical, national, or cultural dimensions).

At the same time, the literature highlights the potential limits of multistakeholderism, particularly its weakness in dealing with sophisticated strategies managed by informed

or powerful stakeholders or coalitions. The absence of formal authority may undermine democratic and public accountability (unchecked authority).[37] The cost of being active—or even involved—in discussions and proposing amendments leads to participants having to choose the norm-setting or policy dialogues in which they should invest. The result is adverse selection: only the most interested stakeholders are involved in each debate, which can cause warring standards or coalitions that impose their preferred compromise (regulatory arbitrage). These players also tend to become agenda setters, initiating a forum when they want to promote a particular solution. The absence of centrality or a hierarchy of norms results in bypassing strategies: players interpret regulatory resistance as harmful and route around it so as to implement their preferences for alternative norms (authoritarian end run). Coalitions can also be formed because players might prefer inclusion. In open processes, self-designated leaders may emerge in loose communities and negotiate with their counterparts to mutually establish and reinforce their respective leadership positions. The result is the formation of "heterarchical" systems that neither guarantee reliance on the most sophisticated skills, nor the consideration of relevant interests. Social scientists have often pointed out the difficulties in scaling up processes of deliberation within participatory networks to large and heterogeneous communities (see, among others, de Moor, 2022). Moreover, manipulation of these open processes might turn them into instruments of hegemony.[38] Carr (2015) notes, for instance, that civil society remains relatively disempowered among Internet governance stakeholders in spite of its important legitimizing role for other groups, namely the technical community, business organizations, and governments. Broadly, these reflections offer a basis for the analysis that follows of the practical implementation of multistakeholderism in Internet governance.

3.3 A Fragmented System under US Leadership

To begin, Internet governance is not a pure model of multistakeholderism. Of course, a set of ODIs are at the center of the governance complex (cf. § 2.3 and note 22). However, other types of organizations and networks are involved in the polycentric system of governance (cf. § 2.2 and note 27).[39] As noted by Carpenter (2013), among others, this leads multistakeholder institutions to coordinate, and sometimes to negotiate, with intergovernmental organizations or industry standardization bodies. Moreover, the existence of several forums is strategically used by actors to advance their specific interests through forum-shopping and forum-shifting. In other words, the bureaucratic and diplomatic decision-making processes characteristic of intergovernmental organizations can be relied upon to influence the dynamic of open standardization in the Internet realm.

Furthermore, according to the "pure" logic of multistakeholderism, governments should not be involved in ODIs since they are not consistent with direct/unmediated democracy, or the representation of interests. Indeed, national governments were not initially supposed to play a role in ICANN. However, in response to demands by the European Commission and the Australian government in the late 1990s, a Governmental Advisory Committee (GAC) was established and added to ICANN's organizational structure, while only conceptualized as a forum for communication between governments and limited to an advisory function. In the same vein, the Internet Governance Forum (IGF) was established in 2005 by the executive branches of several countries as a result of concerns over the dominant role of the US in Internet governance. This led to the creation of a governmental forum to complement the multistakeholder forum in the process driven by the United Nations (Denardis and Raymond, 2013). Of course, national governments have no mandate to negotiate under either arrangement, and cannot impose any decision, but they are involved in and can intervene in the interactions among stakeholders.

Of no less importance is the way the Internet governance ecosystem is organized and performs in practice. Since it is mostly based on pragmatic arrangements rather than any formal mechanism that guarantees representation and consideration of all the relevant stakeholders, it benefits those who designed the initial system and have retained control of its evolution—namely, a web of US governmental agencies and corporations. The ICANN is not the product of any international negotiations, and works without statutes, bylaws, or identified constituencies (Cerf et al, 2014). Vint Cerf—one of the founders of the Internet (see notes 60 and 63), who played a prominent role in ICANN's governance—stated that ICANN sees itself as a governing body without any constitution, since reaching a consensus would be impossible. ICANN performs therefore according to rules adopted under the principle of rough consensus, combined with a web of commitments (with other organizations) and self-established processes of accountability. The IETF is built on the same logic. It is organized around 125 open working groups operating in seven areas (applications, Internet, operations and management, real-time applications, security and transport) However, there is no membership, no fees, and 'nothing to sign' in order to step in (Froomkin, 2003).

Taylor (2015) discusses in detail the major issues raised by ICANN's lack of status or a constitution. First, these keep the organization from establishing any principle of membership, which leads to its directors being de facto appointed by their predecessors and peers, while also blurring the notions of fiduciary duty, the interests of its constituencies, and the public interest. The board is left to review its own decisions, with no external mechanism in place to recall individual directors. It also has total discretion over suggestions made by the working groups that create proposals, and is not

answerable to any higher body. The board is not run on a voluntary basis, but rather employs 15 people that may be remunerated for their work, who act in the interest of the ICANN community rather than for the broader Internet ecosystem.[40] These issues are reinforced by the fact that ICANN derives significant revenues from domain name registration and renewal fees paid by registries and registrars. These revenues are used to fund the organization's operations and to subsidize participants involved in ICANN-related activities and sister organizations like the Internet Society (ISOC). ICANN is also a significant contributor to other governance and policy dialogue fora such as the IGF and NETmundial. This is thus a system without checks and balances.

Moreover, the reform implemented in 2016 to guarantee greater transparency and accountability did not, in fact, significantly change the nature of this highly self-reproducing system of governance. ICANN remains a US legal entity, with internal processes and a legal status that allow the US government, through the NTIA, to prohibit ICANN from acting against the country's well-being (Morten Haugen, 2020). In practice, the governance system in place favors US interests, both through the direct influence of the US government and its federal agencies as well as through a collection of large US corporations (Carr, 2015). Moreover, many members of the so-called 'technical community' are software engineers employed by big tech firms, whose jobs involve actively contributing to open-source software development, open standardization processes, and participating in the networks and ODI involved in Internet governance. Of course, these engineers are not necessarily US citizens, and their formal mandate may not include representing their employers. Yet, they potentially entrench rather than balance the power of the US State and the influence of big tech on Internet governance. Corporate influence also comes from Internet and online service providers responsible for the technical implementation of governance measures (Zalnieriute, 2019), where the binding role and sometimes extraterritorial reach of US legal and political preferences cannot be denied.

On the governmental side, US influence is not exercised unilaterally, but rather through a coalition that includes other Western governments and industry. Throughout ICANN's numerous transitional periods, the US government has increasingly favored a governance regime based on respected tech experts in an effort to stay at arm's length from the organization and ensure its independence from other governments oversight. Multistakeholder rhetoric has also been employed to veto any initiative aimed at transferring given levers of power to foreign governments or intergovernmental organizations (IGOs). Rather, the US government, as the initiator of the Internet, has consistently claimed that its preferred governance model is in line with the traditional US approach of minimizing regulation in a free market-driven economy and decentralized governance. At the same time, its ownership of the addressing system and its

technological leadership have allowed the US government to shape the ICANN's evolution. Officially, the government's role was to allow the multistakeholder community to establish a credible and sustainable system of governance. Though European policymakers would likely have set up ICANN in a different manner, possibly including more public accountability to counterbalance corporate interests, they have consistently supported the US position throughout various reforms (Taylor and Hoffmann, 2019). This dynamic triggered the formation of a coalition of Western states, which has played an active role in ensuring the acceptance of US leadership by the various Internet governance ODIs.[41] Such a position was taken by European countries both due to an alignment of core values and because doing so places them in a position to negotiate support. This has also allowed them, over time, to sideline developing countries and, even more explicitly, China and Russia (see, for instance, Sieckmann and Triebel 2018 or Morten Hauger 2020). In sum, ICANN is a central node in the system of Internet governance, and while it is currently independent of any formal ability of governments to influence its decisions, the US government remains the ultimate guarantor of ICANN's existence and ability to operate.[42]

Broadly, we are witnessing a situation in which the traditional multilateral system of governance over a global infrastructure comprising shared capabilities among private operators and independent nations—embodied in the ITU—has been sidelined by a private organization, ICANN. Its status, bylaws, and membership were never formally negotiated or approved by any organization or government, but rather established under the auspices of a single State. The next section delves into the history of both organizations in an effort to understand how this came to be.

4. How Did We Get Here?

The declining influence of the ITU and the greater profile of ICANN as an alternative can be explained by two broad trends: the digitization of information and communication technology (ICT), and the rising political polarization within the UN system, particularly between the West and developing countries. The digital revolution in IT led to a rethinking of the role of governments as central players in the technical standardization process and in the regulation of service provision and innovation. Moreover, the rise of an infostructure supporting the provision of a wide set of services and multiplying the activities performed online led to a dramatic increase in the diversity of the interested parties in the regulation of e-communication networks and supported services. This challenged the traditional institutions responsible for the governance of

telecommunications systems. At the international level, the balance of power shifted towards a multilateral system due to the enfranchisement of former colonies and, subsequently, the end of the Cold War. This allowed for the formation of coalitions aimed at eroding the leadership of Western nations, especially the US, leading to an organizational lock-in that prevented the ITU from adapting to the new reality. The US government reacted by exploiting the opportunity provided by the invention of the Internet on its own soil. Namely, it proposed both a specific technology and an associated mechanism of governance that served to advance its soft hegemony.

I begin with a brief overview of the history of the ITU, showing the way in which it was progressively sidelined in the governance of international telecommunications infrastructure. This is followed by a return to the history of the Internet in an effort to describe the circumstances under which the ODIs were established and sponsored at the international level. Finally, I highlight the unintended consequences of the current model of governance, in particular the permanent threat of security failures and the fragmentation of the digital space.

4.1 Rise and Decline of the ITU

The history of the ITU[43] is clearly demarcated into two visions associated with two different periods. From its emergence in 1865, as an arrangement among European governments to facilitate transnational telegraphic communication, up until the 1970s, the organization proved capable of adapting to progressively new technologies (e.g., telephony, radiocommunication, satellite communication). It was also able to expand its membership (to almost all existing states) and reorganize to accommodate change (e.g., during the postwar rise of the UN system), as well as reconcile the organization's intergovernmental scope with the participation of the private sector. Of course, its first century of history did not follow a linear path, with several conflicts emerging between nation states regarding the organization's political governance or the regime of access to resources—specifically, the radio spectrum and satellite orbits (e.g., Slotten, 2013)—as well as technical standardization and tariffs. However, until the early 1980s, most players were in a relatively symmetric (while unbalanced) situation. Governments considered telecommunications to be a public good, the provision of which should be publicly supervised. Hence, a national (public or private) telecom operator and, for the largest countries, a national equipment manufacturer were tightly linked to each government. In this context, the ITU was the arena in which deals had to be made between sovereign states. From the 1980s on, however, this situation changed and the ITU gradually became sidelined as a "convergence" occurred between telecommunications, information processing, and media. New players with different views of the government-industry relationship entered the game, and Western

governments embraced novel approaches to regulation in an effort to cope with the pace of innovation and the multiservice nature of e-communication systems. This triggered a clash between a free-market approach to the globalization of digital services and the interconnection of national communication systems under the purview of sovereign states.

The digital transformation was a major game changer. It turned telecommunication networks into components of a broader digital infrastructure in which software became the key technology. This had a major impact on the logic of standardization and resource allocation, since software can extend physical and material limits. Take, for example, a transmission channel, whether radio- or cable-based. Its band is limited, but software can be relied upon to compress the signal and to mix various information streams at the same time, de facto expanding its capacity. Software-based communication radically changed the nature of telecommunications networks, challenging traditional telecommunications governance and regulation.[44] To this regard, Ryan (2012) shows the way in which it clashed with the logic of an organization like the ITU. With regard to radio-spectrum management, a political/territorial approach contrasted with a techno-economic one. The former considers the radio spectrum to be a finite resource and focuses on distributing frequencies within a particular territory to eliminate interference. Meanwhile, the latter seeks to optimize spectrum use by implementing innovation, which requires a light-touch regulatory approach and increased liberalization in order to encourage innovators to develop and implement their creations with the goal of market rewards.[45]

In addition, the fact that the new digital infrastructure became integral to the provision of multiple services meant that a variety of industries and players were affected by telecommunications network governance. These included information systems and service providers, the entertainment industry, and the media, as well as, of course, a multitude of industries once e-commerce started to develop. This called for significant adaptations by the ITU to accommodate new, more diverse, stakeholders (several of which operated across national boundaries), who had a variety of business and technological profiles that had little in common with telephone operators. Moreover, the ITU found itself having to manage the high pace of innovation that characterizes the digital transformation. At the same time, large users and service providers called for greater liberalization of telecommunications markets, since they desired a seamless digital infrastructure to accommodate the globalization of value chains and markets. Under pre-existing trade agreements, specific regimes were in force for telecommunications services, intellectual property, culture and services, which were considered to be totally separate from trade in goods. This resulted in an extreme fragmentation of markets across countries and industries. Liberalization was expected to increase the bargaining power of large users—including online service providers—vis-à-

vis telecom operators and therefore to lower tariffs and guarantee higher service quality and access to their infrastructure. It was also seen as a channel to pressure existing domestic regulatory frameworks to accommodate the provision of information and transnational services (Cowhey and Aronson, 1991).

The digitization of the IT industry meant thus the end of scarcity, provided technological innovation could be accommodated, resulting in a push for the liberalization of markets to allow entry and incentivize innovators and investors.[46] The political dynamics of the post-war period, however, prevented the needed reform of the ITU from occurring. Originally, the ITU was essentially a 'club' of telecommunications operators and governments that sought to harmonize the conditions of interconnection and interoperability across national telecommunications networks (i.e., technical standards and tariffs) and to define the conditions of access to shared resources in the international space, particularly the radio spectrum. The founding conventions were signed by states that had very similar, though sometimes conflicting, interests. In the postwar period, the extension of membership to the newly independent former colonies progressively transformed the organization. These countries gradually reoriented themselves away from their former colonizers, forming a coalition in the spirit of the movements of the 1970s and 1980s aimed at rebalancing international relations and the postcolonial economic order. Since the ITU was an IGO based on the principle of "one state-one vote," the coalition became majoritarian, progressively taking control of the organization and its agenda to implement a decision-making process deemed favorable to the majority. Their outlook was twofold. First, in regulatory matters concerning international telecommunications, the bloc had a strong preference for the status quo, namely a logic of reciprocity among national and public telecommunications operators. This was seen as a source of significant rents for governments.[47] Moreover, the liberalization of telecommunications, both at the domestic and international levels, was considered to favor large corporations from the North to the detriment of building capabilities in the South. The developing countries' second overarching goal was to build these capacities and to rely on the ITU in order to benefit from transfers of technology and expertise from the most developed countries. This resulted in a significant misalignment of interests between, on the one hand, the ITU's ruling coalition, and on the other, Western nations. Since the digital revolution had been largely driven by the US, it was the most affected by the blockage within the ITU and therefore attempted to bypass it. This strategy was made possible by the technological convergence reducing the centrality of the ITU, which was unable to exercise any veto capability. To illustrate this, I describe that which occurred in the three areas in which the ITU is most active: the 'regulation'[48] of international services (tariffs and access to markets), the technical standardization process, and development and technical assistance policies.

The initial convention, signed in Paris by twenty European States in 1865, was meant to replace a web of bilateral agreements on transnational telegraphic communication. It established the technical conditions for network interconnection and communication (including standards such as Morse code) as well as the uniform tariff to be charged for international services and the operating procedures to settle accounts.[49] The early development of radio communication triggered another international convention beginning in 1906 to manage access and sharing of the international space, i.e., the radio spectrum. Since a standards war limited communication across systems, security issues arose in maritime communication—e.g., failure in organizing the rescue of the Titanic—and rules of fair access to the technology had to be agreed upon (Codding, 1991).[50] For a long period of time the regulatory role of the ITU was confined to this relatively light harmonization of tariffs and service conditions across national operators and the rules of access to the international space. The ITU principles and processes were thus originally developed to deal with a relatively stable game (Rutkowski, 1991). Yet, a call by countries with liberalized domestic telecom markets to adapt the international institutional arrangement to the evolving market structure and technology disrupted this status quo (Woodrow, 1991; Ypsilanti, 2013; Fontaine-Skronski and Rioux, 2015).[51] In the late 1980s and early 1990s, the opening of telecommunications, media and online service industries, which began with the breakdown of the AT&T monopoly and the Bell system in the US in 1984, led several Western countries, under US leadership, to liberalize the international telecommunications regime and facilitate access to domestic telecommunications markets. Encountering strong resistance against reforms to the ITU, the US adopted a strategy of forum-shifting (Braithwaite and Drahos, 2000) by including telecommunications on the agenda of the GATT negotiations on the liberalization of services (Uruguay Round).[52] The US rationale for relying on the GATT negotiations was that they provided a framework with negotiation principles and effective tools to implement trade liberalization. The proponents of including telecommunications in the Uruguay Round were also attracted by the dispute settlement procedures available in the GATT/WTO (Bronckers and Larouche, 2007). This move undermined the ability of the ITU to define the transnational telecommunications regime.

Standards are of paramount importance to the telecommunications industry because of the required interoperability among components of the information and communication systems. Depending on the conditions of access to technology—which depend on intellectual property regimes as well as access to industrial know-how—the standards affect the competitive positions of firms and nations. The ITU was progressively sidelined in the process of international standardization since agreements were reached in other fora, even if subsequently formally rubber-stamped by ITU (Besen and Farrell, 1991).[53] More generally, beginning in the 1990s, global standard-setting in the ICT industry

moved beyond the sole purview of the 'Big Three': the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the ITU.[54] Numerous industry consortia, mostly based in the US, emerged and competed with the Big Three, resulting in a paradigm shift (Liu, 2014). Standardization switched from a de jure process oversighted by governments (and diplomatic negotiations) to a de facto process based on voluntary cooperation among industry players disciplined by market competition and adoption by users.[55] The drivers of this change were numerous. First, the expansion of network functionality and the diversity of plugged-in technologies resulted in an explosion in the number of interfaces in which interoperability had to be guaranteed. Second, the pace of innovation required shorter and more flexible standard-setting processes. Third, liberalization generated a global market of equipment and services, requiring a setting of global standards. Fourth, an ideological shift occurred with the development of open innovation processes and peer production, where engineers established de facto standards in a cooperative manner (since access to the technology is open).

The ITU was thus progressively sidelined—both intentionally and unintentionally—in its core function of establishing an international governance regime for telecommunication and standardization. To add to this, a third factor also played a significant role in convincing the founding countries to allow its marginalization. Historically, the ITU was essentially aimed at providing a technical basis for transnational communication and reducing transaction costs among network operators. The new majority decided in the 1980s to significantly transform the organization's purpose and logic. This began in the form of a battle over its organizational logic,[56] which had initially consisted of a small secretariat responsible for rationalizing the back-office governance matters concerning a set of conventions on contrasting issues. The related areas—tariffs, spectrum, etc.—were therefore managed in a relatively decentralized manner, following a strong pragmatic and engineering logic. In contrast to the proponents of this loose federal structure (i.e., US and the West), the new majority favored a major centralizing and unifying reform, which was passed in an extraordinary plenipotentiary conference held in 1992. Moreover, appointments to key executive positions and boards became based on election by the member states, whereas previously there had been a separation between the rules for executive and technical appointments and political bodies. In addition, the composition of boards and councils became systematically based on geographical representativity, mechanically resulting in a reduction of North American and European influence.[57] Then, this reform further designated development support as one of the three central purposes of the ITU. The work of the Union was thus organized into three bureaus: Radiocommunications, Telecommunications Standardization, and Development. This move was strongly opposed by the US government and other Western states, since it

transformed the organization into an instrument of redistribution from North to South. Moreover, development support would reliably oppose liberalization of the telecom sector through a rhetoric of supporting nascent industries.[58]

The combination of these elements resulted in the sidelining of the ITU, largely explaining the failure of the WSIS and the Dubai conference. Nowadays, the ITU no longer plays a significant role in Internet governance, instead declaring its "commitment to work with the Internet community and extend the benefits of the Internet to all global citizens."

4.2 The Disruptive Invention of the Internet…and the Battle over its Governance

The rise of the heterarchical ecosystem at the center of Internet governance is hardly the result of a harmonious process of "organic" development, as it has rather been marked by major clashes among diverging interests. The US federal administration has proven to be agile and ingenious in exploiting opportunities rather than attempting to steer the whole process. It was able to identify the prospects provided by end-to-end technology at an early stage and, later on, to exploit the associated mode of multistakeholder governance as an alternative to multilateralism. Indeed, the Internet itself was not invented, nor even planned, by the US government or its Department of Defense (DOD). Rather, it is the result of a set of innovations made by computer scientists working in university laboratories and funded by DOD grants.[59] These laboratories were initially motivated by the need to share scarce computer capabilities and to coordinate their work, which led them to develop solutions to organize communication among computers and among themselves. This grew into the set of Internet principles and technologies—developed between 1969 and 1984—that were recognized by the military as holding promise for the development of resilient communication systems, though the DOD accomplished this by forking. The development of the technology was then pushed forward in an academic context with funding from the National Science Foundation in 1985.[60] The latter soon realized that the potential of the technology could only be realized if it was opened up to industry funding and technical capabilities, especially from the computer and software industries. This resulted in the Internet becoming available to non-academic players and for commercial use from 1992,[61] which came about through an active policy of technology transfer and cooperation with industry from 1988.

Until the mid-1980s, the Internet was a rather small network (111 hosts in 1977, 1000 in 1984). It then grew exponentially (100,000 hosts in 1990, 1 million in 1992, 2 billion in 2001). The agencies governing the Internet were thus established in this context of explosive scaling-up of the network and constant changes in its purpose and reach, along with cumulative innovations in multiple directions.[62] The Internet of the 1980s and early

1990s was governed by the academics who had been active at its origin, often in a very informal way. The expansion of the network required formal management of the addressing system and protocols. Moreover, the principles had to be operationalized through service provision, especially the root server of the Internet. The technical community established organizations (IAB, IETF, IANA) in the realm of academia, with little regard for the legal foundations of the pragmatic, informal arrangements established within a small community sharing a common technical and political culture. The US government, for its part, delegated the functions over which it had control, as the initial sponsor of the Internet, to universities. In particular, the management of the addressing system was contracted to the Information Science Institute within the University of Southern California, which in practice fell to Jon Postel.

The decision to open the Internet to commercial use triggered a conflict between the proponents of an open and non-commercial Internet and those who saw the Internet as a new technological system with immense potential for users and businesses, though one whose development required significant investments and further innovation. Furthermore, as the Internet became accessible to non-American users outside of academia, tensions arose between supporters of a fully global Internet and those who preferred an international approach that recognized state sovereignty; a viewpoint advanced at the time by European governments and Australia. In an uncertain political and legal environment, the technical community at the origin of the Internet called for the "independence" of cyberspace while also seeking to retain control of its technical governance. The latter, at the time, was poorly understood by both policymakers and business leaders, with only a handful of US federal agencies and industrial corporations—along with the Internet's "founding fathers"—understanding the matter in great detail.

The Internet Society (ISOC) was established in 1992 by Vint Cerf to allow the technical community to keep control of the standardization process (which was the purview of the IETF) and the addressing system (then under the auspices of the IANA). This triggered a battle among three main groups: the technical community and civic activists, who advocated for an Internet free of governmental and business influences; industry groups, which pushed for an Internet that could secure private investment and allow the development of e-commerce (as it had begun to be called) through secure property rights and a borderless Internet (capable of sustaining self-regulated and tax-free exchanges at the global level); and governments, which were interested in the promises of the digital infrastructure while seeking to safeguard their sovereignty. Commercial interests opposed the transfer of IANA to ISOC. Meanwhile, the fact that ISOC had been established in Switzerland—with the clear aim of establishing itself in a non-US jurisdiction in order to coordinate with international organizations like the ITU (Heath, 1997)—did not please the US government (Mueller, 2004; Wu, 2008; Datysgueld, 2018).

The latter went on to sign a five-year contract in 1993 for the management of the root servers of the addressing system with a private service provider: Network Solutions Inc. (NSI), later renamed Verisign. At the time, Jon Postel's legitimacy carried such weight that USC was kept on as a policy coordinator (IANA function), also under a five-year contract. The federal decision and its implementation were, however, severely criticized[63] and the coming of an end to the two contracts in 1998 set off an extraordinary institutional battle,[64] accompanied by political, civic, and academic controversies. The US government proposed the formation of a new entity — the ICANN – to control the DNS root, under the condition that it would be a US-based non-profit, while inclusivity towards the international community would be fostered in the norm-setting process (Wu, 2008).

In parallel to this trend, IGOs and foreign governments entered the game. Beginning in 1992, conflicts surfaced around the registration of names in the DNS that were identical to registered trademarks. These had sometimes arisen by accident (names related to local brands that were registered trademarks in other jurisdictions), while in other cases there was a clear will to capture the benefits of well-established brands (cybersquatting). This led the International Trademark Association (INTA), an NGO representing trademark owners, and the World Intellectual Property Organization (WIPO) to push for regulations concerning the distribution of domain names (cf. note 29). As the Internet started to become international, there was also a call to create national addressing systems. Given the stakes, an interim ad hoc committee (IAHC) was formed in 1996 by IANA, IETF, ISOC, INTA, WIPO, and ITU. It resulted in an MOU in May 1997 on the principles to be followed to create new generic and national domain names. A month later, the Clinton-Gore administration published a paper on its vision of Internet development and the role of for-profit organizations and e-commerce, raising tensions over Internet governance. This was the first step of an offensive to stop the conflict by providing a solution.

In the spring of 1998, the US government published green and white papers on its strategy for transferring the expiring contracts with NSI and USC to a new entity. That summer, the bylaws of ICANN were drafted, with an innovative governance structure (Board, Supporting Organizations, Advisory Committees, and Constituencies) that placed governments in an advisory position. An Interim Board met in Cambridge in November, adopted the bylaws, and entered a contractual relationship with the NTIA and the Department of Commerce (DOC). In March 1999, the first ICANN meeting was convened in Singapore, followed by the election of the board members in the summer of 2000. The latter was the subject of significant controversy, leading to the first of a series of reforms of the ICANN.[65]

Once ICANN was established, it was strongly backed by corporate players. The technical community gradually came to realize that it largely remained in the driver's seat. NGOs and activists, as well as non-Western governments, became active supporters of reforms within ICANN, though their main efforts consisted of calling for an alternative to ICANN, especially during the WSIS meetings in Geneva and Tunis in the early 2000s. However, the divergences among international organizations like the ITU, authoritarian governments, and anti-globalization activists were too strong for them to agree on or propose a common alternative. Thus, Western governments, industry players, and the technical community formed a coalition that de facto supported ICANN as the second-best solution as long as its organizations and processes would be reformed to accommodate their claims. This was fully in line with the preference of the US government, which subsequently relinquished sovereignty in favor of a solution that would allow it to preserve its fundamental interests and keep the other governments in an asymmetric situation.

Clearly, the US government was able to play its own game since it "owned" the Internet. It had an interest in keeping all players on board as it needed the inventiveness and the expertise of the technical community, the resources and the promises of industry, and the benefits of being the sponsor of global infrastructure. The country managed this by accommodating certain elements from each of these conflicting groups; ICANN and its design were the solution proposed and implemented. In turn, the organization maintained a low profile so as to avoid the forking of significant players.

4.3 Internationalization of the Internet: the Hegemon's Gift

While not specifically invented as a tool of soft hegemony, the US government recognized the international potential of the Internet after noticing its economic promise in the mid-1980s. With the end of the Cold War, the Clinton-Gore administration proposed spending the "peace dividend"—the money no longer required for maintaining military equilibrium with the USSR—on research and development, with the specific goal of promoting a digitalized information infrastructure to support sustainable growth based on innovation, while also strengthening US competitiveness in IT.[66] This strategy was articulated through two actions by the federal government. The High-Performance Computing Act of 1991 was based on the idea expressed by Vice President Gore to the US Congress that technology was one of a nation's endowments that could, like natural resources, generate wealth and power. However, technological resources are created through human endeavor rather than extracted from nature. Therefore, the private sector should be incentivized to develop this resource (see Car, 2015). The "Framework for Global Electronic Commerce," a white paper published in 1998, reaffirmed the centrality of the private sector in the development of the Internet. The

latter was seen as a key step towards a global marketplace where transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller resided. It was furthermore argued that this marketplace should not be regulated by governments, whose role should rather be limited to ensuring competition, protecting intellectual property and privacy, preventing fraud, fostering transparency, and facilitating dispute resolution. The US government expressed its will to keep the Internet (and related transactions) free of tariffs and taxes, and its desire to support the development of an uniform international commercial code, as well as claimed that self-regulation should prevail in order to effectuate market transactions and preserve trust in online activities.

The US government, thus, sponsored the development of Internet technology with an understanding of its usefulness as a tool to restore the competitiveness of US industry. In doing so, it also fostered its worldwide adoption. The open-source nature of the core software resources facilitated adoption by new users including individuals, firms, and governmental organizations. Furthermore, the end-to-end nature of the network boosted positive network externalities. When the Internet was made available to global users, it also came with a portfolio of technologies and services provided by a constellation of US corporations, which had benefited from technology transfers and support from the US government through the country's financial industry. Ostensibly, the US government applied the principle of viral marketing—which had been invented in the 1990s by new entrants in digital markets—at a macro level. It did so by "subsidizing" adoption through free access to components of the service in order to trigger positive network externalities among and between adopters and service providers, and then securing lock-in effects based on users' investments in the technology (David, 1985; Katz and Shapiro, 1998). The sponsored technology came bundled with both an economic and a governance model, which were, in a sense, embedded in the technology. The end-to-end architecture was consistent with the model of a free-market economy as well as with the model of platforms necessary for online transactions (Rochet and Tirole, 2003; Brousseau and Pénard, 2007). Protection of the global nature of the information space and market infrastructure also required a light-touch approach to regulating online activities. Given the potential for absolute enforcement through the addressing system and communication protocol, it was crucial that the governance of core Internet resources remained immune to (foreign) governmental influence. Hence, the governance regime had to be bundled with the access to the technology, which was possible due to the self-enforceability of norms embedded in digital code.

Thanks to its clever and agile strategy of supporting Internet development and diffusion, the US government ensured the victory of its domestically developed standard over its main competitor, the X.25 protocol developed by the ITU (Abbate, 1999; Townes, 2012,

Chenou and Radu, 2014). Before the commercialization and popularization of the Internet in the 1990s, traditional telecommunications operators created the X.25 standard to support communication between computers in administrated networks. It was used in the development of the earliest generation of online services, such as computer reservation systems (CRS) or the French Minitel. It was also behind the information system of many organizations and the exchanges of information between them (e.g., interbank payments and clearing, EDI support for value chain logistics). Indeed, such administrated networks are secure. The diffusion of the TCP/IP protocol associated with end-to-end architecture relied on the will of users and their investments in the technology, not on telecommunication operators' willingness to allow the provision of innovative services. It subsequently benefited from increasing returns to adoption once a critical mass had been guaranteed by the incubation and subsidized adoption of the technology by the US government.

This strategy was advantageous to the US in several ways. The "neutrality" of the network guaranteed a level playing field for the introduction of new services (DeNardis, 2014). The mixture of libertarianism, anti-authoritarianism, and pro-entrepreneurial beliefs associated with the Internet's "open" character and "distributed" architecture, aligned with the core "liberal" values of Western societies (Lewis, 2010). The associated multistakeholder model, which seemingly sidelined bureaucracies and politicians in favor of governance driven by scientists[67] and citizens went hand in hand with rising skepticism against corrupt political elites and cynical intergovernmental relations. At the same time, the Internet was an acceptable solution for "closed" organizations and foreign governments since the e2e principle allowed for the creation of all kinds of restricted access networks (both private and governmental), allowing users to (partly) escape US control.

Clearly, the so-called multistakeholder model, combined with the de facto veto power of the US government, enabled the latter to retain control of the evolution of the Internet architecture and governance while maintaining a very low profile. Acting in this manner helped to ensure the Internet's acceptance by foreign governments and a wide array of stakeholders.

4.4 The 'Built-in' Limits of the Current Governance Model

While the US strategy has successfully brought about the global adoption of an infrastructure and associated governance regime favorable to own its interests, as well as has provided global users with a set of essential benefits in terms of low cost, rapid innovation, development dynamics, and operational scale, this success has come at a price. The decentralized adoption by users pre-empted negotiations between incumbent

economic and political players, resulting in the absence of constitutional agreements (e.g., if not a hierarchy of norms, at least a mechanism to settle disputes) that the constituencies of the global information infrastructure might abide by. Furthermore, the implemented order tends to be minimal, as it would be extremely costly for the "center" to implement common norms given the scope of activities on the network and the heterogeneous preferences and beliefs of users. Thus, many missing links remain in the governance of online activities. Furthermore, new technological opportunities tend to be embraced by those seeking to destabilize the current order rather than improving it, resulting in threats and system risks.

The fundamental limit of the current governance arrangement lies in the ability of any coalition to fork if they feel that their preferences and needs are not accommodated at the system level. Defectors generate losses in terms of network externalities borne by the whole community of Internet users. Two forces tend to cause or exacerbate failures in contemporary Internet governance. First, the success of the Internet in terms of its plasticity and performance has resulted in it supporting a growing set of human and social activities, raising the sensitivity and the stakes for questions of governance. The sovereign states' ability to set rules has increasingly been challenged, sparking conflicts. Moreover, the success of platforms and other Internet ecosystems has tended to generate new players that put traditional rulers to the test. Second, the absence of agreement on the current model of governance—perceived to have been unilaterally imposed to the benefit of some—has led certain players to employ strategies aimed at weakening the existing framework. These efforts center on attempts to fragment Internet governance (through multiple fora) and the infostructure, resulting in losses of connectivity and security, as well as reducing quality in a general sense. The remainder of this section further develops these reflections.

As noted by Broeders (2015), with the Internet becoming the locus of an increasing number of activities, issues of sovereignty have grown in importance for governments. Increasingly, the latter have come to view control over the network's activities as a legitimate means to achieve their policy ends. Furthermore, the politico-philosophical foundation embedded in the e2e architecture, which prioritizes concepts such as human rights, freedom of speech, civil liberties, open competition, and freedom of entrepreneurship, comes into conflict with many socio-political arrangements and governmental preferences across the world. Tension can also arise between national security and the integrity and security of the network, since national governments might be willing to exercise surveillance (generating incentives for users to hide their behaviors) and might develop tools for offensive strategies (such as vulnerabilities inserted into software) as both preventive and retaliatory weapons. The combination of these behaviors has a propensity to undermine the consistency and security of the Internet.

Indeed, these principles of universality, interoperability, and accessibility, which lie at the heart of the Internet, are fundamentally at odds with those of national sovereignty inherited from the Westphalian order. From its inception, cyberspace was designed as a space beyond the authority of States (Barlow, 1996; Wu, 1997), with significant implications for the ability of states to control cross-border information flows or to exert authority within territorial borders (e.g., Betz and Stevens 2011, 55–74). The need to cooperate in order to tackle challenges raised by online activities such as security, market regulation, or taxation requires States to "pool" their sovereignty. Yet this comes at a cost in terms of governments' ability to control affairs within their own borders, and to make decisions on important aspects of their national legislation. For fear of jeopardizing sovereignty, many States refuse multilateral modes of cooperation, leading to a fragmented system of global governance.[68] This fundamental clash is obviously accentuated in States that do not embrace Western values.[69] The result is a lack of cooperation and a set of unilateral measures that damage the integrity and reliability of the global infostructure (Broders, 2015). Such measures range from censorship and surveillance to attacks aimed at incapacitating servers. Moreover, the concepts of "technological sovereignty" or "data sovereignty" have gained prominence in the context of efforts to re-territorialize online activities. Though the official reasons given for such measures are to protect citizens, in practice they serve to restore governments' capacity to control online activities and exert pressure on service providers. These efforts clash with the fundamental logic of the Internet, which seeks to use the available (communication and information processing) capabilities on the network to optimize service quality.

The presence of large platforms and Internet intermediaries raises another issue. As noted by Elkin-Koren and Perel (2022), among others, governments rely on Internet intermediaries to implement their legal orders in the online realm. There has thus emerged situations of mutual dependence: governments rely on the the capabilities of large players to control users' behaviors. On the one hand, a hierarchy between the public and the private order persist, since governments of sufficiently large countries and economies — says the G20—are able to harm such intermediaries. On the other hand, when governments request that intermediaries control online activities, they are de facto asking them to bypass the privacy regulations that the governments themselves have put in place. Moreover, citizens and corporations are submitted to a (private) administrative order that no longer guarantees due process. Ultimately, since it can be complex and costly for intermediaries to enforce the diverse array of local regulations, they tend to pressure governments to implement de facto uniform regional or global norms. This not only runs counter to state sovereignty, but it also leads large online platforms and ecosystems to behave as sovereign entities with de facto legitimacy to control online

operations. The integrity and the neutrality of the network is thus affected, as is its ability to be self-governed. Large platforms tend to benefit from unbalanced power, raising questions about their impact on fair competition and capacity to control entry and innovation (Parker et al., 2022).

Another source of weakness in the current governance architecture of the Internet lies in its built-in web of interacting regimes. As noted above, traditional multilateral mechanisms (IGOs) were sidelined rather than dismantled entirely, and their endorsement was sought for the emerging multistakeholder organizations (ODIs). Today, both types of organizations continue to operate in a hybrid, coopetitive manner that ensures mutual perpetuation. This situation has been exploited by competing sovereign states, which actively practice forum-shopping and forum-shifting,[70] resulting in a fragmented and inconsistent governance system characterized by missing links, overlapping norms, fuzziness, and risks.

The challenge of security is, to this regard, emblematic. Conflict between cybersecurity and national security has led to a situation of fragmented governance. As a result, security threats have become embedded in the infrastructure of the Internet itself. The use of cyberspace as a field for international conflicts and as a tool for population control (mass surveillance, control of information, campaigns of disinformation, etc.) has detrimental effects for global cybersecurity.[71] Indeed, there is a link between national security policies and security breaches. In the name of national security, individuals and private operators have limitations into their encryption capabilities, and vulnerabilities are implemented in the hardware and software of the Internet. The purpose of these policies is to allow governments to monitor online activities, or to carry out invisible actions on the "dark web."[72] In this respect, the Snowden revelations not only undermined the credibility of the US as a guarantor of the integrity of the system[73], but also boosted other governments' online hacking efforts. The Internet is insecure not only because governments use it as a battlefield, but because the built-in weaknesses are exploited by all kinds of players for purposes of fraud or crime. Given the level of risk—including threats to critical infrastructure—several initiatives have been developed at the international level in an attempt to regulate cyberconflict and foster inter-governmental cooperation against crime.[74] Unsurprisingly, the absence of a shared approach to the issue has prevented the formation of any consensus; even in terms of the laws of war or descriptions of the "territory" to be regulated.[75] Today, cybersecurity is managed by "defense" alliances and informal pragmatic arrangements involving the private sector that seek to detect and respond to attacks and threats.[76]

Beyond the negative impact of the lack of security on the costs and benefits of on-line activities, many governments rely on security threat arguments to press into service UN

Charter protections guaranteeing member sovereignty, territorial integrity, and political independence. This strategy is implemented as a shield against the principle of universality, interoperability, and accessibility attached to the Internet. Such an approach clearly conflicts with the principle of net neutrality, which prohibits network operators from prioritizing or blocking the delivery of certain types of traffic or content. Indeed, compromising net neutrality can jeopardize the overall quality of the Internet through fragmentation.[77]

The forces driving fragmentation and the emergence of development gridlock weaken the claim that US dominance has been effective at guaranteeing the stability and unity of the Internet (Rogers, 2007; Taylor and Hoffmann, 2019). In short, the fragmentation of the Internet, brought about in part by the increasing number of public and private gateways, reduces connectivity and the open character of the Internet, which may inhibit the pace of innovation and the expected effectiveness of the selection process. Likewise, fragmentation in Internet governance leads to missing links that subvert several features of the network, especially in matters relating to security. This in turn has implications for its ability to support economic and civic transactions, strengthening traditional rulers and intermediaries to the cost of boundaries and the capture of rents.

5. An Opportunist and Agile Strategy to Establish a New Approach in International Governance

How, then, should this history of Internet governance be interpreted? To better understand the dynamics at play, I now attempt to provide an explanation of the events surrounding the battle for legitimacy. As observed by Scholte (2019), legitimacy is a polysemic notion open to many approaches. In an institutional economics context, I embrace the view proposed by Greif and Rubin (2014), who consider legitimacy to be one of the channels through which a ruler's authority is recognized, allowing it to impose order without resorting to force or threats.[78] To a large extent, the maneuvers by the US government can be interpreted as a strategy to legitimize a governance arrangement that was more in line with US interests than a possible alternative. The strategy was one of adhesion rather than constraint, since any coalition was able to fork, and a multitude of state and non-state actors could and did erect barriers and gateways to cordon off sub-sections of the information space. I begin by considering this very point, before

turning to how the ICANN was instrumented by the US to propose an alternative to multilateralism.

5.1 Three Paths

Three alternative paths have been proposed in the literature on Internet governance to explain the dominant position taken by the US. The first might be termed the "imperialist scenario," which posits that the US government sabotaged the ITU in order to impose a technology with embedded tools to ensure its dominance. This vision is in line with the "military origin" of the network, the in-depth involvement of federal intelligence and security agencies in the development of the Internet, and cooperation between the US government and industry groups to allow the latter to dominate service provision and control the progress of the technology. In contrast, the second path proposes the "intrinsic superiority of multistakeholderism." It reflects the beliefs of the designers of the Internet—as well as those of many global activists and libertarians—who see governments as seeking to control public opinion, or even ensure the subservience of the populace. In this view, the usual game played in international relations is a clear example of cynical bargaining among entities that are bent on disregarding, or even damaging, the collective welfare. Multistakeholderism, then, despite its limits, would have won a competition between the models. This new model emerged out of the battles over governance of digital infrastructure precisely because the technology allows its users to implement the underlying principle of direct democracy and self-organization. This led to the formation of a governance system in which imperfections can be fixed pragmatically thanks to its fundamentally polycentric and open nature. The third path interprets the history of Internet governance as occurring under a "US soft-hegemony scenario." In this view, the US government incubated a technology in line with its strategic interests, recognizing its potential if adopted at the global level due to positive network externalities. It then sponsored the adoption of the technology while stewarding its progress in such a way as to protect one of its central features—end-to-end architecture—which maximizes the network externalities from both a static (i.e., diversity and quality of services) and dynamic (i.e., pace and diffusion of innovations) perspective. This approach offered additional benefits, such as US industry benefiting from a first-mover advantage and a furthering of US political interests through the values spread by the technology, as well as the associated economic, social, and political model being consistent with the views of most of the countries' educated elites.[79]

While certain facts support each of these scenarios, some are more easily refuted than others. The imperialist scenario, for example, is countered by the fact that the US government was unable to use force to impose its technology and governance model on adopters. Indeed, even its closest allies resisted the liberal approach to regulating

telecommunications, the distributed network architecture, and the governance model that sidelined governments. These features ran counter to their historic approach, their industrial competitive advantage, and their social-democratic inclination. Strategic competitors of the US and developing countries, meanwhile, were also quite opposed to the US preferences, and have continued to resist them. In addition to these players failing to form a coalition to provide an alternative, the ITU gradually became weaker through a combination of political and bureaucratic drift. Most importantly, the US government and industry groups accommodated several of the claims of their opponents, denigrators, and competitors. The "victory of multistakeholderism" viewpoint is vindicated by strong governmental involvement - by the US, European nations, Russia and China, among others - as well as the participation of IGOs in policy debates and the daily governance of the Internet. As demonstrated in this chapter and in the literature, the claim that the open commons was built using an open consensus-building process free from state interference is not entirely accurate. Rather, it is clear that the US government retained control of the process, even if it did not monitor all aspects of it, and remains able to this day to veto certain potential changes in the system. Moreover, the most powerful states are currently engaged in pressuring, or even forcing, technical intermediaries to follow regulations (e.g., in security-related or competition matters), as well as playing games in various Internet governance fora (from the ITU to the policy cooperation alliance mentioned above).

All of these elements, however, are compatible with the "soft hegemony" scenario. As mentioned, the US government has engaged in a strategy of taking the lead in Internet governance, while managing to keep the various stakeholders involved in a concentric system that favors some (e.g., the technical and US business community) more than others (e.g., foreign governments). It has, meanwhile, ensured sufficient benefits from network externalities to all parties to deter forking. In governance matters, concessions were made to accommodate the most vocal claims, such as the creation of the GAC within ICANN, and the representation of 'users at large' on the ICANN board. Most importantly, the US government refrained from abusing, at least openly, its dominant position - with the notable exception, of course, of the PRISM surveillance program - in order to keep an opposed coalition from forming. The move toward greater formal independence for ICANN was clearly a response to Edward Snowden's revelation of the exceptional asymmetric power the US wields over the global communication system. From a technical perspective, moreover, the technology had the strong advantage of allowing the creation of a variety of private or governmental virtual networks and other information spaces that are outside the influence of the US government and domination by US industry.

5.2 ICANN as a Tool of Soft Power to Steer Global Digital Governance

In the context of this 'soft hegemony' scenario, it is interesting to analyze the strategy employed by the US government to establish its legitimacy, allowing it to exercise stewardship over Internet governance. As observed by Greif and Rubin, from an 'instrumental' viewpoint, legitimacy can be considered as a shared belief among those who are ruled that the demands of a ruling authority should be obeyed because the latter has the "right" to govern. By motivating compliance, legitimacy can substitute coercive power and thus reduce governance costs. Legitimacy can then be understood as one "ingredient" of a player's ruling capabilities, and the later can therefore deliberately seeks to establish and reinforce it, even if legitimacy can also draw from it the very pool of talent from which the leadership of ICANN was drawn s own intrinsic characteristics. When the ruler is an individual, legitimacy may derive from his or her identity, perhaps as a member of a dynasty, or from his or her skill as a benevolent and effective leader. In the case of an organization, as noted by Scholte (2019), legitimacy may be derived from its procedures (transparency, effectiveness, non-discrimination, etc.), performance, purpose, or ability to exercise leadership. Greif and Rubin point out, however, that legitimizing agents are essential to inform the beliefs of the ruled. A ruler's intrinsic characteristics and their alignment with the expectations of those they rule could be sufficient for a ruler to attain "cultural" legitimacy. If not, the ruler should build "institutional" legitimacy through recognition by independent and credible third parties. Such independent agents may help grant leaders legitimacy in exchange for policy concessions or partitioning of policy space in their favor.

Applied to this context, the situation of the US was one of low ability to impose its authority since forking and exit options were accessible to many players, and since it benefitted from a poor cultural legitimacy as a sovereign state ruling unilaterally an international regime. Thus, US efforts to guide the evolution of the Internet and its governance had to be legitimized by third parties.

In the first round between the US government and ISOC, industry groups were the legitimizing agent of the US government. Yet, this was not sufficient since ISOC, led by the technical community, had secured the support of several IGOs. The US government therefore had to exercise its authority by refusing to delegate the management of the addressing system to ISOC. The creation of ICANN, meanwhile, was a way to concede power to the technical community and (some) foreign governments. However, the concessions—and the stakes—were clearly different in the two cases. In practice, the

pool of talents from which the leadership of ICANN was drawn is made up of mostly US citizens employed by US corporations or universities. The technical community therefore received much of the power and influence it had sought when establishing ISOC. This provided a blueprint for managing the second round between the US government and the UN multilateral system, embodied in the ITU. The existence of ICANN, its independence from the US government and its cooperation with IGOs were the policy concessions required to achieve legitimacy among a heterogeneous set of stakeholders: the business and technical communities, Western governments, and a set of IGOs.

This quest for legitimacy also explains the rhetoric and institutional strategies that have been developed around ICANN. A strong ideological campaign has been orchestrated to build and defend the model of multistakeholderism as a superior system for dealing with governance issues, especially in the context of cultural diversity and absence of (global) government. This is paradoxical since the same proponents of this view have repeatedly defended the idea that Internet governance was in fact a low-profile technical matter. Meanwhile, ICANN has updated its mission statement to include compliance with human rights and democratic principles, with the clear aim of morally legitimizing its purpose. The organization has, in addition, been the subject of a permanent policy dialogue and reforms aimed at enhancing the transparency of its processes, its operational effectiveness, and its independence from the US government.[80] There is a clear logic of establishing its intrinsic legitimacy in the long run, combining a rhetoric of accountability and effectiveness. Overall, the ODI system has been able to manage a permanent scaling up of the Internet, an explosion in its uses, and stability of its critical resources. It has done so while also accommodating the preferences of many stakeholders and relying on revenue from the DNS to fund civic initiatives supporting a sustainable growth regime. There is thus a clear will to establish the legitimacy of ICANN on procedural, performance, purpose, and relational grounds.

6. Conclusion: An Open-Ended Process Based on the Dynamics of Adhesion vs. Splitting

According to Greif and Rubin, the English Reformation reduced the legitimizing power of the Church, leading the Tudor monarchs to increasingly rely on Parliament as a legitimizing agent. They therefore enhanced the power of Parliament and its secular components, bringing about an endogenous change in the balance of political power in

England. This was the primary source of an open-ended evolution that saw the dynamic development of Great Britain with the Industrial Revolution and parliamentary democracy. The recent history of Internet governance is similarly the result of an institutional strategy, here aiming to promote a governance arrangement that would reinforce US leadership of the global order, a role the country has sought throughout the postwar period. Certain political concessions were needed to stimulate adoption by users and to involve the technical and business communities in the development of the system. Moreover, the ability of users, large technical intermediaries, and sovereign states to fork led the US to adopt a low profile. While this has resulted in certain failures (i.e., in matters of security, network integrity, monopoly power, etc.), it has also maintained US soft hegemony and the country's continued oversight of the development of the Internet.

Indubitably, there are costs, born in part by the users who do not fully benefit from the promises of an open, fully distributed, and multi-purpose infostructure. Intermediaries and sovereign states tend to undermine the network and online activities. These groups do, of course, have incentives to keep the resulting fragmentation of the Internet at a "reasonable" level; all gatekeepers balance their capability to capture rents with the necessity of creating value through network externalities. The US Government also bears part of the cost, since it will have to relinquish sovereignty in a permanent "constitutional bargain," as discussed by Brousseau et al. (2010; in the context of the building of national orders), triggering an open-ended process of institutional evolution.

This evolution will depend on four groups of actors, who are, in practice, playing different games. States and governments will continue to challenge US leadership, though will likely remain unable to reverse the latter and implement a multilateral system. That said, there will be a permanent call for greater multilateralism in Internet governance; likely counteracted by efforts to bolster the legitimacy of multistakeholderism. The second group comprises the network of transnational elites who support multistakeholderism: academics, business leaders, civil society activists, government agency employees, and members of the technical community. They will be the principal supporters of the current model of governance as long as they continue to derive social prestige, power, and money from it. These actors will also have to avoid excessive capture of rents and misbehavior if they are to keep their legitimacy. In addition, they will experience strong pressure to rationalize and clarify the current organization of ICANN and its satellites. Third, corporations, especially technical intermediaries and large platforms, will support any changes that are favorable to the ongoing commodification of digital resources, especially data. This is the key to building new business models and enhancing existing ones, enhancing the so-called customer experience (while locking them in). At the same time, their position is precarious due to the threat they represent to open competition and personal privacy, which may result in governmental regulations in response to

citizens preferences, thus jeopardizing their ability to advocate for a light-touch approach in the governance of economic affairs on the Internet. Indeed, governments must balance their citizens' demands for regulation with the significant investments made by industry. Finally, the "end users" play an essential role in the Internet governance ecosystem by granting legitimacy. They may very well call for the decision-making process to be less vulnerable to capture and manipulation by the ODI system. End users might also favor the enactment of Internet bills of rights and guarantees of the rule of law, which would lead to a greater hybridization between new and emerging ODIs and traditional political and judicial authorities

Footnotes:

[1] Another much considered model is polycentrism, a model in which problems—even transnational ones—must be pragmatically addressed through direct co-operation by the relevant (public) authorities rather than being mediated by the sole national governments. Polycentrism is envisioned as allowing agile management of trans-territorial and trans-sectoral issues in an environment of overlapping mandates, ambiguous hierarchies, and the absence of a consistent supreme authority to manage trade-offs. This model has been extensively studied in the context of environmental and natural resource challenges.
Both polycentrism and multistakeholderism are considered as variations within the approach of international relations in terms of global governance, which highlights why the traditional approach of international governance should be surpassed. Global governance is associated with three features (Rosenau & Czempiel 1992; Rosenau 1995; Dingwerth 2008; Weiss & Wilkinson 2014; Liaropoulos, 2016): a shift of regulation from the national level to levels beyond the state, the emergence of non-state actors alongside the states (Nye & Donahue, 2010), and the recognition of the legitimacy of rules that have been agreed upon in a decision-making process that meets reasonable standards of inclusiveness, transparency and accountability, even if not enacted by national governments.

[2] It is instructive to differentiate five phases in the history of the Internet, corresponding to changes in its nature. From 1957 to the late 1970s, it was a tool aimed at facilitating the sharing of scarce computing capabilities, relied upon for military research. In the 1980s, the tool was made available to the US academic community. The Internet was then opened up to commercial usage in the early 1990s, triggering the development of online services. In the early 2000s, the Internet began to support media and platforms aimed at exchanging and sharing information. From 2010, with the spread of mobile communication and smartphones, the Internet became a tool to deliver all kinds of customized services, as well as sparked the development of the Internet of Things, which link computers and receivers implanted in all kinds of equipment, supporting a wave of generalized automation.

[3] The number of Internet users is difficult to calculate. In 1981, there were fewer than 300 computers linked to the Internet, and still less than 90,000 by 1989. By 1993, over 1,000,000 computers were linked, while as of 2020, there appears to be some 4.833 billion Internet users. These consist of about 2.525 million users in Asia (penetration rate of 42.2%), 728 million in Europe (87.2%), over 566 million in Africa (42.2%), 467 million in Latin America and the Caribbean (71.5%), about 333 million in North America (90.3%), 184 million in the Middle East (70.8%), and 28 million in Oceania (67.7%) (Internet World Stats, 2020). The number of Internet hosts grew from 10 in the early 1970s to around 100,000 by 1990, and is now more than 1 billion (source: Hobbes' Internet Timeline,
https://www.zakon.org/robert/internet/timeline/Count_Host-log.gif, last accessed Dec. 2020)

[4] In fact, the International Telecommunication Union (ITU) was only established in 1932 in Madrid, when the Telegraph Convention of 1865 (amended in 1885 to include the telephone) and the Radiotelegraph Convention of 1906 were combined into a single convention embracing the three fields of telegraphy, telephony, and radio. In 1947, the ITU became a branch of the UN system and moved its headquarters to Geneva. The current organization and work of the ITU is based on Convention of the International Telecommunication Union adopted in 1982 in Nairobi by 190 states. The convention legally defines the goals of the ITU, its organizational structure, and its operations. It is supplemented by the Administrative Regulations, which govern special procedures. The highest-ranking offices of the ITU (Council and Secretary-General) manage the daily operations of the organization and prepare the principles and general conventions to be amended and voted by Plenipotentiary Conferences or World Conferences (ITU 2011). The maximum number of individuals on the Council is equal to 25 percent of the total number of member states; the Council is elected by the Plenipotentiary Conference with due regard to the need for equitable

distribution of Council seats among the five world regions. Corporations and Partner Organizations must pay a membership fee and do not have any decision-making rights. They are involved in working groups and committees aimed at preparing decisions and designing standards.

[5] At the Plenipotentiary Conference, members vote on the composition and organizational structure of the ITU, decide on its financing, and revise the wording of official documents, if necessary. In the subordinate study and working groups, technical questions are addressed on a regular basis and the resulting conclusions are published as recommendations, resolutions, or other policy guidelines. These gain binding character only after their adoption by the Plenipotentiary Conference or by unilateral endorsement of national governmental agencies.

[6] The Internet was developed by software developers and computer scientists working in universities on projects funded by grants provided by the US Federal Government (see note 60). The initial purpose was to develop resources to manage more efficiently the scarce computing capabilities available in the 1970's and 1980's, and to support coordination among researchers and teams. The individuals involved in this endeavor established themselves as a community, cooperatively managing the Internet and its process of development. Once the Internet was made available to a broader community of users, this community both welcomed a wide set of new contributors (for instance employed in the industry and in the government) and established itself as being one of the legitimate "stakeholders" of the governance of the Internet. In particular, it started considering itself as the "guardian" of the founding technical design of the Internet, also associated to a political project carried out by some of the founding fathers of the Internet (see note 33).

[7] In practice, ICANN has never made such a decision, since it was not the technical implementer of its decisions. The addressing system of the Internet, rather, is technically implemented by Verisign, a private corporation that holds a contract with the US government. Until the transfer of IANA functions to ICANN in 2016, the US federal government, through its contract with Verisign, had ultimate authority over the Internet's entire navigation system. Thus, ICANN never had to act in its capacity as a last-resort body to ostracize any Internet user. The US government did so on several occasions, the two most famous being the US invasion of Iraq in 2003, where critical communication resources in Iraq were disconnected, and in 2012 when the US Department of Justice disconnected Megaupload servers that were considered to be resources relied upon by pirates to infringe copyright laws by massively sharing protected content. On the other side, ICANN decisions were never, at least publicly, vetoed by the US federal government (Teleanu, 2016). Though, the relationship between ICANN and the US government was always asymmetric, with ICANN lacking the power to make truly independent decisions prior to 2016 (Brousseau, 2007; Jayawardane et al., 2015; Kruger, 2016).

[8] Cf. for example Resolutions 73 and 113 of the ITU in 2002.

[9] "While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors. At their annual meeting delegates discuss, exchange information and share good practices with each other. The IGF facilitates a common understanding of how to maximize Internet opportunities and address risks and challenges that arise"
(https://www.intgovforum.org/multilingual/tags/about, last accessed Dec. 2020).

[10] Epstein (2013) discusses the creation of the IGF as a compromise between the multilateral and multistakeholder approaches of global governance. The WSIS was marked by the official inclusion of non-state actors in discussions as legitimate contributors to the global communication policy (Raboy et al., 2010). While UN processes had previously placed civil society organizations in advisory capacities at the edges of formal processes, WSIS participants from civil society took part in the core conversations (Raboy and Landry, 2005; Raboy et al., 2010). This, however, resulted in quite confusing discussions, which led to the establishment of a Working Group on Internet Governance (WGIG), tasked with developing a working definition of Internet governance, identifying policy issues that should come under its umbrella, and

mapping the roles of various stakeholders (United Nations World Summit on the Information Society, 2003, para. 13b; see also Kleinwächter, 2008; Mathiason, 2009; Mueller, 2010). The group was organized by the Secretary General of the ITU, which gave it the legitimacy of the UN in spite of the disparities in formal status between the state and non-state actors. The conclusion of these discussions was that they should be continued, which led to the creation of the IGF. As pointed out by Taylor & Hoffmann (2019), as a forum for dialogue, the IGF was deliberately kept separate from the UN bureaucratic machinery. As a consequence, it has always struggled financially, which, along with its loose mandate, might explain its poor performance.

[11] In the context of the WSIS, a vast coalition of non-state actors, both commercial and non-commercial, were de facto aligned with US opposition to the state-centric approach to Internet governance. Epstein (2013) highlights the various clashes around the vision of the governance of the global order in general and the global infrastructure that marked the WSIS discussion. For the promoters of a vision based on sovereign states, the ITU Plenipotentiary Conference was a more favorable arena since only governments have a say in the final decision.

[12] A 1998 Memorandum of Understanding between ICANN and the National Telecommunications and Information Administration (NTIA) of the Department of Commerce (DOC) initiated a process intended to transition the management of the addressing system of the Internet to a private not-for-profit entity. While the DOC played no role in the internal governance or day-to-day operations of ICANN, the US government, through the DOC/NTIA, retained a role with respect to the DNS via three separate contractual agreements: a 2009 Affirmation of Commitments (AoC) between the DOC and ICANN; a contract between ICANN and DOC to perform various technical functions such as allocating IP address blocks, editing the root zone file, and coordinating the assignment of unique protocol numbers; and a cooperative agreement between DOC and VeriSign to manage and maintain the official DNS root zone file. As observed by Kruger (2014), by virtue of the three contracts, the United States government - through the DOC/NTIA - exerted legacy authority and stewardship over ICANN (see below). Moreover, since the NTIA was the lead agency overseeing domain name issues, other federal agencies maintained a specific interest in the DNS that potentially affected their missions. For example, the Federal Trade Commission (FTC) seeks to protect consumer privacy on the Internet, the Department of Justice (DOJ) addresses Internet crime and intellectual property issues, and the Department of Defense and Department of Homeland Security address cybersecurity issues. However, none of these agencies had legal authority over ICANN or the running of the DNS.

Briefly returning to the three contracts:

- The purpose of the 2009 Affirmation of Commitments (AoC) was to "institutionalize and memorialize" the technical coordination of the DNS globally through a private sector-led organization. The AoC replaced the previous Memorandum of Understanding and subsequent Joint Project Agreement between DOC and ICANN. Under the AoC, ICANN committed to remain a not-for-profit corporation "headquartered in the United States of America". The AoC established a review panel (including the Administrator of the NTIA) aimed at periodically making recommendations to the ICANN Board about its organization and policies.
- The IANA contract between ICANN and the DOC specified that the contractor must be a wholly US-owned and operated firm or a US university or college, that all primary operations and systems shall remain within the United States, and that the U.S. government reserves the right to inspect the premises, systems, and processes of all facilities and components used for the performance of the contract.
- Meanwhile, the cooperative agreement between DOC and Verisign authorized the latter to manage and maintain the official root zone file that is contained in the Internet's root servers that

support the functioning of the Domain Name System. By virtue of these legal agreements, the DOC had to approve changes or modifications made to the root zone file.

[13] IANA, the Internet Assigned Numbers Authority, is an administrative function of the Internet that keeps track of IP addresses (the identification of connected devices), domain names (the identification of online service providers), and protocol parameter identifiers (language identification) that are used in Internet standards. Regardless of the type of identifier, the IANA function ensures that values are managed for uniqueness and made available in publicly accessible registries so there can be no confusion. In short, IANA's role is to manage and ensure the global uniqueness of Internet identifiers, guaranteeing the openness of the system and its end-to-end architecture.
On March 2014, NTIA announced its intention to transition IANA to "the global Internet multistakeholder community," and made clear that it would not accept any transition proposal that replaced the NTIA role with a government-led solution or one located within an intergovernmental organization. For two years, ICANN engaged in a process to develop a transition proposal that would meet the NTIA criteria. On March 10, 2016, the ICANN Board formally adopted a transition plan, which was approved by NTIA on June 9, 2016. On September 30, 2016, the contract between NTIA and ICANN expired, thus completing and implementing the transition.

[14] For an overview, see, in particular, Kruger (2016), Hill (2016), Raustiala (2017), Snyder et al. (2017)

[15] The Snowden revelations triggered the organization of an international conference in Brazil entitled the NETmundial in May 2014 (interestingly, held at the invitation of the President of Brazil and the CEO of ICANN; while the ITU convened the WSIS on behalf of the United Nations system). This São Paulo "Global Multistakeholder Meeting on the Future of Internet Governance" resulted in the publication of a set of (non-binding) recommendations, known today as the São Paulo Principles. The later attempt to defend the initial principles around which the Internet was built (e.g., uniform and unfragmented cyberspace, open and distributed architecture, stability and resilience of the network, etc.), respect humanist values for users (especially fundamental rights and multiculturalism) and govern under the tenet of multistakeholderism. These principles were themselves in line with the Montevideo Statement published in October 2013, which synthesized the recommendations of the "technical community" on Internet governance. Thus, the reorganization of ICANN was in many ways a timely response to pressure from important stakeholders in the Internet governance system.

[16] Indeed, when millions and billions of digital devices are interconnected, there are scarcity issues in terms of computing and communication capabilities that require the provision of services by intermediaries specialized in providing the ability to access the communication infrastructure and to distribute communication flows among available capabilities. This is the role of specialized routers, internet service providers, and backbone operators, which manage the routing space to optimize the management of communication flows, and route aggregation (i.e., to manage the scarcity of addresses IP numbers are distributed by blocks to ISPs and provided to users on a temporary basis; by DHCP). All are in a position to favor certain users, type of flows, and even to block some exchanges due to their content, or the identity of users, which would violate the e2e logic, hence the necessity to "neutrally" manage the network.

[17] The notion of "users" encompasses any user of the Internet, whether an individual or a public or private organization, who uses or delivers a service of any kind over the network, including communication management (e.g., social networks), intermediation (e.g., online platforms), or direct provision of content and tangible services (by monitoring physical and human capabilities).

[18] As discussed in Brousseau and Marzouki (2012), among others, there is naturally also a possibility to bypass the encoded rule by hacking the code. This results in the recursive effect between code and law: the enforceability of code should be guaranteed by a legal ban on hacking and pirating, which must be translated into technical principles to guarantee compliance, and so on. This discussion was initiated by

Rotenberg (2001) and Wu (2003), who wrote about the roles of code and law in compliance or avoidance of regulations.

[19] As recalled by Datysgeld (2018), the concept of modeling the network into an "open, minimalist, and neutral" space was initially consolidated within the US federal system of research and funded by the Department of Defense. The open nature of the Internet informed the US military's decision to fork (see note 24) into its own network, leaving the fate of ARPANET to the academic community (funded by the National Science Foundation). Internet working among an increasing number of universities prompted the development of the Internet Protocol Suite (TCP/IP), while the benefits in terms of network effects boosted its adoption by an increasingly diverse and international set of users. This bottom-up process of development and adoption helped it win the standard race against the top-down Open Systems Interconnection (OSI) protocol that was championed by the ITU and the International Organization for Standardization (ISO).

[20] The critical resources of the Internet are made of the registries (see note 14), which allow ensuring the uniqueness of identifiers (i.e., "numbers" for the devices, and addresses for the applications ran on the Internet, and protocol parameter identifiers for the instructions to the interconnected devices and applications), and of root servers that distribute these registries to all users to guarantee the operation of the Internet and on the Internet.

[21] Organically developed institutions (ODIs) include the Internet Corporation for Assigned Names and Numbers (ICANN), Regional Internet Address Registries (RIRs), the Internet Engineering Task Force (IETF), the Internet Society (ISOC) and the World Wide Web Consortium (W3C).

The Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF), housed within the Internet Society (ISOC), are responsible for the core Internet protocol standards, while the World Wide Web Consortium (W3C) deals with the protocols and standards of the World Wide Web.

The IETF is an open standards organization, which has no formal membership roster or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors. The IETF started out as an activity supported by the US Federal Government. Since 1993, it has operated under the auspices of ISOC.

The World Wide Web Consortium (W3C) was founded in 1994 by Tim Berners-Lee after he left the European Organization for Nuclear Research (CERN). It is responsible for developing standards, protocols and guidelines for the Web in order to guarantee compatibility among the software and services. The Consortium is jointly administered by the MIT Computer Science and Artificial Intelligence Laboratory in the US, the European Research Consortium for Informatics and Mathematics (ERCIM, hosted in France), Keio University (in Japan) and Beihang University (in China). The Consortium is funded and governed by its membership, which include businesses, nonprofit organizations, universities, governmental entities, and individuals.

[22] According to Vincent and Camp (2004), the contrasting approaches to standardization between traditional standard-setting organizations (like the ISO or the ITU) and the communities involved in the digital standardization, which work under the umbrellas of organizations like the W3C and the IETF (see note 22), differ in the specificity of the object of the standardization process: material realization vs. software. The latter is operational as soon as it is designed and can also be tested at relatively low cost and almost just in time. Richardson and Eberlein (2011) similarly point out that standard-setting organizations in corporate finance need to have their standards endorsed by public authorities, since the latter must guarantee enforcement of last resort and ensure that these standards are compliant with the law. Digital standards do not need to be approved since they are self-enforceable through technological compatibility.

[23] In the software environment, a fork describes a code that is split into two (or more) identical copies on which additional development is performed, typically to carry out different tasks. The two software versions then diverge and can no longer share the same code/add-ons. They might even lose any capability of interoperability. In the context of a digital network, forking will imply the development of two alternative addressing systems and a contrasting evolution of the communication protocols. This ability to fork in the absence of a "supreme court" responsible for guaranteeing the network's integrity and benefits to all — i.e., the network externalities of a borderless and seamless universal

network — is the reason why network fragmentation is feared by many promoters of the Internet. See I.a. De Vey Mestdagh and Rijgersberg (2010).

[24] An abundant literature is dedicated to the many stakeholders and issues involved in Internet governance. These include Mueller, 1999 and 2010; Brousseau et al., 2012; Choucri, 2012; Deibert, 2013; DeNardis, 2014; Nye, 2014; West, 2014; Jayawardane, et al. 2015; Cornish, 2015; Denardis and Musiani, 2016, Kruger (2016), Datysgeld (2018). For detailed descriptions of the Internet technical governance system, see ISOC (2014), Cerf et al. (2014), and Taylor and Hoffmann (2019). There are also many online resources available on the sites of the main ODIs involved in the system.

[25] Among the stakeholders that are crucial in this process, those that control the technical operation of the networks play a particularly important role. These include the owners and operators of servers and networks, domain name registrars and registries, regional IP address allocation organizations, standards organizations, Internet service providers, and online service providers, whose decisions to adopt standards and comply with principles have a major effect on all users.

[26] A wide set of fora are involved in Internet governance:

- First, there are standardization organizations. Internet standards organizations include the Internet Engineering Task Force (IETF) hosted by the Internet Society (ISOC), the Internet Architecture Board (IAB) and the World Wide Web Consortium (W3C). However, beyond the dedicated organizations, a wide array of other standard-setting bodies deals with issues that affect the operation of the digital infrastructure and are therefore involved in the standardization process. Some are recognized international fora backed by governments, even though industry players are involved in the working groups of the ITU (for telecom) or the International Organization for Standardization (ISO). Many others are more or less formal and more or less global standardization arrangements established by the industry, with a strong leadership role played by the tech giants. For example, The Institute of Electrical and Electronics Engineers (IEEE) is a US based professional association, which objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering and similar disciplines. The Institute of Electrical and Electronics Engineers Standards Association (IEEE SA) is an Operating Unit within IEEE that develops global standards in a broad range of industries. Tech firms often employ a mixed strategy: sitting in standardization organizations and also attempting to establish de facto standards by implementing them in their products and promoting adoption by users.
- Second, there are intergovernmental policy forums. Governments attempt to coordinate policies, or at least to voice their perspective in fora that vary in their degree of formality and inclusiveness. At the core of Internet governance lies the Governmental Advisory Committee (GAC) established within ICANN to "provide advice" to the ICANN Board on matters of public policy, Membership in the GAC is open to all national governments that wish to participate. Interestingly, the GAC does not host only sovereign states. Its members can be national governments, multinational governmental organizations, treaty organizations, and "public authorities." The Internet Governance Forum (IGF; cf. notes 10 and 11) is the other pillar of policy dialogue with a specific track dedicated to intergovernmental dialogue. Its purpose is to be a platform of discussion open to all interested parties. The IGF's mandate does not include hosting negotiations or making formal recommendations to the UN system. This is because many intergovernmental organizations host negotiations themselves. Mention has already been made of the role of the International Telecommunications Union (ITU), but the World Intellectual Property Organization (WIPO), World Trade Organization (WTO), Organization for Economic Co-operation and Development (OECD), the United Nations Educational, Scientific and Cultural Organization (UNESCO), as well as many regional organizations have also been involved. All these IGOs are concerned with the adaptation of the transnational regime they oversee to the Internet era. More generally, they attempt to deal with conflicting legal norms and cooperation in legal enforcement. The significant cultural and political clashes, reinforced by economic and sovereignty competition among nations, result in very slow progress in these parallel discussion fora. Thus, many "minimal coalitions" emerge in attempts to impose regional or targeted norms (for instance, in matter of cybersecurity or cybercrime; cf. note 75).
- Third, many fora consist of groups of non-state actors. Business associations such as the ICC, WEF, WITSA, CCIA and GNI are also active in organizing dialogue among their stakeholders with the aim of being able to promote agreed upon principles in technical or policy fora. The same occurs with NGOs and civil society players, which attempt to build coalitions at the international level. Both business associations and civil society

coalitions are active in the above-mentioned policy dialogue platforms hosted by IGOs; their involvement has been analyzed by, among others, Weiss et al. (2009), Tallberg et al. (2014) and Levinson & Marzouki, (2016), who highlight the fact that IGOs evolved from coordinating mechanisms among nation-states to platform organizing interactions among governments, civil society organizations, the private sector, and other stakeholders such as the technical community; IGOs no longer being the univocal way to settle transnational regulations, but rather simple "political opportunity structures" (as described by Talberg et al., 2014). This increasing partnering between IGOs and non-state actors is linked to the broadening of the issues at stake and the necessity for IGOs to benefit from expertise on a wide set of issues (e.g., Levinson & Marzouki, 2016) and manage informal processes that run parallel to official ones. These activities help IGOs to achieve their goals despite diplomatic blockage (due both to their focused mandate and to clashes over sovereignty; see, e.g., Schemeil 2012; Hoogue et al., 2019)).

[27] The transfer of IANA functions from the NTIA to ICANN reinforced the centrality of ICANN in the core technical governance of the Internet. Indeed, the "communities" involved in the management of numbering and protocols have always had semi-autonomous relationships with ICANN. One of the aims of transferring IANA functions and the associated reform of ICANN was to prevent the potential fragmentation of the Internet by creating a structure aimed at maintaining consistency between the management of the DNS (naming) and IP addresses systems (numbering) and Internet protocols. Separation would have made it easier for individual numbering and protocol agencies to build out independent sub-networks, while IP addresses, autonomous system numbers, and protocols are likely to increase in significance with future developments such as the Internet of Things.

[28] To avoid cybersquatting, ICANN designed a mandatory process alongside the World Intellectual Property Organization (WIPO) called the Universal Dispute Resolution Policy (UDRP), which regulates trademark and brand disputes. All registrars that distribute domain names must comply with decisions under the policy.

Beyond the WIPO, Chenou and Radu (2014) highlight the way in which major IGOs cooperate with ICANN: UNESCO has worked extensively with ICANN on the internationalization of Internet domain names, while the WTO and the OECD are involved in the Governmental Advisory Committee, etc.

[29] This "low profile" and "technical" character is, however, balanced by the fact that ICANN reinforces its legitimacy by introducing itself as an organization that supports humanistic and democratic values. Morten Haugen (2020), for instance, points out that ICANN itself does not claim to exercise purely technical governance activities, but rather emphasizes its compliance and alignment with principles of human rights and corporate social responsibility.

[30] Manual Castells has pointed out that the strength of the standards based governance is not exercised by exclusion from the networks, but by the logic of conformity that governs inclusion in the network.

[31] There are two approaches to defining ICANN's role as a regulator of the Internet (beyond the technical administration of the addressing system). The first is to consider the role of ICANN as an "economic" regulator of service providers which deliver services linked to the addressing system (provision of IP addresses and domain names). By extension, the ability of ICANN to create scarcity in the number of available addresses and bottlenecks in the distribution system has been scrutinized in a significant body of literature and several controversies (see, for instance, syntheses of these debates in Klein and Mueller (2005), de Vey Mestdagh and Rijgersberg (2010), Mueller and Kuerbis (2014), and Broeders (2015)).

The second approach is to consider the role of ICANN as a decision maker of last resort when questions arise on the inclusion of certain users or communities in the Internet system, which ICANN can deny through a refusal to provide recognition/attribution or addresses. Internet protocols, moreover, can allow classes of usage (and therefore of services). While ICANN is not directly in charge of developing protocols, it decides whether commands are core components of the Internet Protocol (IP), which would make them a legitimate set of instructions recognized by all the devices connected to the Internet. Generally speaking, the norms established by ICANN have a direct effect on the Internet as a whole, since any actor that wishes to take part in the network is obliged to implicitly accept or at least actively engage with the norms. This second approach and the 'political' potential of ICANN has been analyzed by Klein (2002), Brousseau (2007), Christou and Simpson (2007), and DeNardis (2014), among others.

[32] In 1996, John Perry Barlow, the founder of the Electronic Frontier Foundation (EFF) stated the following in "A Declaration of the Independence of Cyberspace": "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one… Cyberspace does not lie within your borders." This approach reflected an era in which online

communities were small, homogeneous, and able to regulate themselves using consensus building and net neutrality. As Barlow phrased it: "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different." Nor was Barlow alone in these views: David Clark of the Massachusetts Institute of Technology (formerly Chief Internet Architect after 1982) defended the principle of rough consensus in open communities of practice in 1992, saying "We reject kings, presidents and voting. We believe in rough consensus and running code." Such statements were behind the analysis proposed by Lessig in 1999 of encoded legal principles and open process of lawmaking.

[33] A significant academic literature is dedicated to analyzing this model, including Drezner (2004), Chenou (2011), Cammaerts (2011), DeNardis and Raymond (2013), DeNardis (2014), Mueller and Wagner (2014), Carr (2015), and Cohen (2019).

[34] Debate between the supporters of the two models has taken place both in the academia and diplomatic arenas, with various contributions made in the different policy fora concerned with Internet governance (e.g., ISOC, ICANN, IGF). In the diplomatic domain, multistakeholderism is supported by Western governments. Of course, even EU member states seek to protect their cyber-borders and data from the surveillance systems of the US (West, 2014) and to impose constraints on big tech (Nocetti 2015). However, they tend to prefer the economic benefits of connectivity to the option of creating national or regional cyberspaces, and attempt to influence the current Internet governance architecture. Carr (2015), for instance, reports the then Communications Minister of Australia, Malcolm Turnbull, as supporting "an open Internet that is administered by multi-stakeholder organizations like ICANN and NOT [sic] by governments." In a hearing on proposed Internet regulation, US Congressman Greg Walden argued that "weakening the multi-stakeholder model threatens the Internet, harming its ability to spread prosperity and freedom." In contrast, non-Western powers tend to support multilateralism. Xi Jinping, President of the People's Republic of China, declared in 2015 that "The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations It covers all aspects of state-to-state relations, which also includes cyberspace.[…] We should respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing."

[35] Interestingly, in recent years, the UN system has tended to support multistakeholderism. This was the case with the WSIS, which was one of the first world summits where civil society was given extensive access to the preparatory process and presence at the meeting, as noted by Cammaerts and Carpentier (2006), and the creation of the IGF, even though no actual diplomatic agreements came out of these processes. In 2019, a UN high level expert group recommended that "as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation," thus appearing to prioritize cooperation over direct governance. The report goes on to express "support a multi-stakeholder 'systems' approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age." The organizational arrangement would be a "distributed co-governance architecture (COGOV) relying "on the self-forming 'horizontal' network approach used by the Internet Engineering Task Force, the Internet Corporation for Assigned Names and Numbers (ICANN), the World Wide Web Consortium, the Regional Internet Registries, the IEEE and others to host networks to design norms and policies. This proposal would extend this agile network approach to issues affecting the broader digital economy and society. It would oversee the "Digital Commons Architecture" and "would aim to synergies efforts by governments, civil society and businesses to ensure that digital technologies promote the SDGs and to address risks of social harm. It would comprise multi-stakeholder tracks to create dialogue around emerging issues and communicate use cases and problems to be solved to stakeholders, and an annual meeting to act as a clearing house." ITU, would thus be totally sidelined if their recommendations were to be followed.

[36] The model does not consider the wisdom of the crowd. Rather, it is envisioned as a way to select the best contribution, with the ideal model for its supporters being the IETF as a true meritocracy: if members of the IETF community determine that an engineer's ideas have value, those ideas are adopted and incorporated into the Internet's suite of standards. Ideas that are dated or counterproductive, on the other hand, fester and fail.

[37] Accountability requires understandability. Digital standards are developed via procedures that involve experts and are encoded in highly technical specifications and algorithms, which are difficult to check and interpret.

[38] von Bernstorff (2003) convincingly highlights the mechanisms at play. First, the network topology tends to sustain the dominance of the most central players. Second, in line with Mancur Olson's logic of collective action, small groups

with a highly focused interest invest more to establish their dominance over larger groups with less-focused interest. Third, as stated by Habermas' conditions for participatory and deliberative democracy, potential participants must be willing to engage actively in discussions on regulatory issues and contribute to the decisions. The fragmentation of debates into a series of highly technical discussions undermines participation. Finally, in line with Gramsci's control of "narratives," the governance solutions most compatible with widely resonant norms like freedom, privacy, democracy, equality and political self-determination have a greater chance of being seen as legitimate. Carr (2015) insists on the performativity of the discourse of legitimization, which allow "a specific group of US government officials, computer scientists, and business people (…) to present its interests as being in harmony with those of Internet users and other national Governments."

[39] This is due to the imperative of interoperability. As pointed out by Carpenter (2013), the IETF's work on Internet protocols only makes sense if the ITU-T defines basic transmission standards for optical fiber, telephony, and so on. In turn, these only make sense if the Internet protocols are there to exploit them. Both organizations understand that in order to meet the needs of industry, it is imperative to quickly resolve differences and avoid duplication of work, a fact that is officially and publicly recognized by ITU officials.

[40] The ICANN structure has two types of stakeholder groups: three Supporting Organizations, namely the Generic Names Supporting Organization (GNSO), the Address Supporting Organization (ASO), and the country code Names Supporting Organization (ccNSO), which are focused on making policy for domain names and IP addresses, and four Advisory Committees that provide advice to the ICANN board, namely the Governmental Advisory Committee (GAC), the Security and Stability Advisory Committee (SSAC), the Root Server System Advisory Committee (RSSAC) and the At Large Advisory Committee (ALAC). The advice of the GAC and other Advisory Committees is not binding on the ICANN directors, though over time the internal rules have strengthened the board's obligation to provide reasons for not following GAC advice. (Taylor & Hoffmann, 2019). Most voting directors are appointed by the Supporting Organizations. Elected members are selected by a Nominating Committee, a specialized body made up of a rotation of individuals that are considered trustworthy by the community (Kwalwasser, 2009).

[41] This observation is the subject of a persisting and vibrant literature about the lack of representative legitimacy in core Internet governance bodies, highlighting the formal and de facto lack of influence by non-Western governments (e.g., Morten Haugen, 2020) and civil society (e.g., Taylor and Hoffmann, 2019); as well as the absence of credible mechanisms aimed at reducing these asymmetries (Malcolm, 2016).

[42] This was a central condition for the transfer of IANA functions to ICANN. Vint Cerf, VP at Google and former Chairman of the Board of the ICANN, even wrote in 2016 about the proposal of the IANA transition to ICANN: "Some fears have been voiced that the complex proposal poses risks that authoritarian governments within the ICANN Governmental Advisory Committee (GAC) or through some external means might wrest control of ICANN from its multi-stakeholder constituencies.[…] I am persuaded the terms and conditions of the proposed operating practices are well protected against such an outcome […] The headquarters of ICANN will remain in the U.S."

[43] In addition to the scholarly literature (in particular Meyer, 1946; Codding and Rutkowski, 1982; Lee, 1996; Lyall, 2011 ; Ryan, 2012; Slotten, 2013; Ypsilanti, 2013), a variety of documents are available on the ITU website, including the reports issued by the Secretariat after each Plenipotentiary Conference, some important milestone reports prepared to inform the Secretariat and the membership when reforms were discussed (e.g. the "missing link report" from 1984), a history of telecommunication and its regulation edited by the ITU and published in 1965, and a collection of the basic texts of the International Telecommunication Union adopted by the 2011 Plenipotentiary Conference. (http://itu.int/go/OverviewITUsHistoryArticle) [last accessed, December 2020].

[44] The use of frequencies for satellite communications was discussed in the ITU and regulated on the basis of the 'common heritage' principle and outer-space law in general, which resulted in significant conflicts between developing and developed countries. Specifically, the principle was viewed as inefficient since it resulted in undue rents to countries that were unable to implement the necessary technology to use those frequencies.

[45] This example highlights how the ITU was poorly "intellectually" equipped to consider Internet regulation. While the Internet has been considered by many to be a "global public good" as well as a "natural resource" or "common heritage," this perspective ignores the need for incentivizing private players to invest in the production of the info-infrastructure and related innovations. Nye (2014) discusses the economic and legal rationale for classifying the Internet as a global commons or public good and the shortcomings of such a view. Cyberspace consists of a global common infrastructure, but it is not a global commons since its infrastructure is mostly owned by the private sector and is located in the sovereign territory of states (Cornish 2015.).

[46] Beyond this approach in terms of political preferences, Weimer (2006) notices that politicians and regulators may prefer delegation of industry standardization, regulation or governance to stakeholders in order to benefit from their expertise, especially in cases of rapid evolution. In addition, doing so tends to protect the former groups from blame in case of failure. This was one of the drivers of the light-touch approach of the FCC in the US, when the digitization of telecommunication networks led to the development of "Value-Added Services," a designation created by the FCC for computer-mediated information services. William Kennard, then Chairman of the FCC, stated later that "The reality is that the Internet grew so fast that policymakers could not have written a code to govern it even if they wanted to." According to analyses by Mueller (2010) and Chenou and Radu (2014), this generated an environment favorable to the bottom-up emergence of ODIs.

[47] Historically, telecom operators viewed long distance tariffs and transnational communication rates as mechanisms to extract rents aimed at funding the "universal service"; i.e., guaranteed access to the local loop at low rates for households.

[48] As noted by Ypsilanti (2013), ITU's main claimed purpose is not to "regulate" the international telecommunication system but rather to "promote", "harmonize" and support "international cooperation," as stated in its constitution. ITU recognizes the "sovereign right of each State to regulate its telecommunication."

[49] By the early twentieth century, the complexity of international telephone service and long-distance telegraphy made it necessary to carry out international studies between Union conferences in order to develop relevant international standards. Two consultative committees were therefore created in 1925: the International Telephone Consultative Committee (CCIF) and the International Telegraph Consultative Committee (CCIT). Each established a structure, with Study Groups carrying out research and developing proposed standards (called Recommendations) and regular Plenary Assemblies that approved the standards and organized the work of the Study Groups. In view of the basic similarity of many of the technical problems faced by the CCIF and CCIT, a decision was made in 1956 to merge the two committees into a single committee: the International Telegraph and Telephone Consultative Committee (CCITT), renamed in 1992 as the Telecommunication Standardization Sector (ITU-T), one of the three branches of the ITU. Its functions are to study technical, operating, and tariff questions and adopt recommendations on them.

[50] ITU's work in the area of radio communications began in 1906 when the first International Radiotelegraph Conference gathered 29 maritime states in Berlin to sign the International Radiotelegraph Convention. In 1927, the International Radiotelegraph Conference in Washington established the International Radio Consultative Committee (CCIR) to study technical and operating questions related to radio communications and to issue recommendations on them. In 1947, the International Frequency Registration Board (IFRB) was created to act as an administrative body to regulate the use of frequencies. In 1992, the CCIR and the IFRB were merged, together with other working groups related to radiocommunication to become the Radiocommunication Sector (ITU-R).

[51] There were different views across nations since various models of "modernization" could be envisaged: a national champion to exploit the rent, a mall model (i.e., a public incumbent challenged and completed by new entrants), or a full competition model.

[52] Initiated in 1989, the telecommunications negotiations in the ITU broke down in the spring of 1996, when the United States bowed out. The US went on to have success with small-scale agreements such as NAFTA, after which it turned to the WTO, where it gained acceptance of the principle of liberalization of services and an Agreement on Basic Telecommunications (ABT) in 1997.

[53] The WTO Agreement on Technical Barriers to Trade (TBT Agreement) requires Members to use relevant international standards as a basis for their technical regulations. The practical question, then, becomes which Standards Setting Organizations (SSOs) qualify as international standard-setting bodies under the TBT. Since they are supervised by governments and IGOs, the ISO, IEC and ITU — qualified as the "Big Three" — are qualified. Other SSOs such as the IEEE also qualify since they comply with certain conditions, regardless of whether their standards are ratified by one of the Big Three. However, not every SSO carries the legitimacy required for the purposes of the TBT. This underscores the importance of cooperating with major SSOs to have new standards approved. (cf note 55)

[54] Until the 1970s, the development of standards in the ICT sector was effectively a monopoly comprised of the Big Three. Within the ITU, the CCITT was run by the national postal, telegraph, and telephone (PTT) firms and Recognized Private Operating Agencies (RPOAs), which enjoyed monopoly power in their respective countries. The ISO and the IEC, both non-governmental organizations, consisted of national members who represented the interests of their countries. The three institutions coordinated their activities to avoid duplication of effort.

[55] The EU and the US clearly have different preferences on the matter: a centralized/publicly sponsored approach is preferred by the EU, a decentralized/market-based approach by the US. The EU standardization system is hierarchical, coordinated and regulated, with standard-setting activities operating within a framework of government oversight. In the US, meanwhile, the private sector has traditionally dominated standardization through competitive market arrangements. (Cf. Winn 2009). Such a divergent approach may explain why most of the de facto ICT standardization consortia did not come from the EU, but from the US.

[56] The 1988 Plenipotentiary Conference organized in Nice was unconclusive. A High-Level Committee (HLC) was established to review the Union's overall structure and working methods and make proposal for reforms, all of which were approved by another Plenipotentiary Conference held in Geneva in 1992, solidifying the grip of developing countries over the ITU.

[57] In 1868, a permanent secretariat was established: the International Bureau of Telegraph Administrations, entrusted with administrative duties. These included gathering and disseminating technical information, publishing rate (tariff) tables, collecting statistics, and publishing a journal on telegraphy matters (the Journal Télégraphique). The Bureau was located in Bern, Switzerland. Its information-sharing responsibilities were relatively limited in order to preserve the sovereignty of the founding states. To deal with technological and commercial change, "Administrative Conferences" were responsible, from 1875, for revising the Regulations and the Table of Telegraphic Rates. They were attended by technical experts from the member states, who did not have the right to revise the International Telegraph Convention itself.

The International Telecommunications Conference, held in Atlantic City in 1947, established the basis of the "modern" IGO on the model of the UN organizations, withs its own bureaucratic and technical capabilities. The conference determined that a Secretary General and staff needed to be appointed to administer the General Secretariat of the ITU and Geneva was chosen as its permanent seat. Progressively, the bureaucratic structure took control of setting the agenda and coordinating the working groups and organizing the Plenipotentiary Conferences.

[58] In 1951, the ITU joined the United Nations Expanded Program of Technical Assistance to contribute its expertise in the telecommunications area. In 1960, a Technical Cooperation Department (TCD) was created within the General Secretariat to foster the establishment and improvement of telecommunication networks in the developing countries. The Department administered programs which sent telecommunications experts to advise and train technicians and engineers. Following a 1984 report by a group of high-level experts known as the Maitland Commission, which highlighted the impact of telecommunications on development, the Nice Plenipotentiary Conference in 1989 established the Telecommunication Development Bureau (in place of the TCD within the Secretary-General) with an elected Director, so as to place technical assistance to developing countries on the same footing as the Union's traditional activities of standardization and spectrum management. The 1992 Plenipotentiary Conference consecrated this change by designating development as one of the three main branches of the ITU.

[59] DARPANET was launched in 1969 as a non-hierarchical network of four connected computers, respectively at the Stanford Research Institute, the University of California Los Angeles, the University of Utah and the University of Santa Barbara. In 1971, Ray Tomlinson established the principle of the email system. The TCP/IP system was invented in 1974 by Vint Cerf and Bob Kahn and allowed a transition from connecting computers to connecting networks. The Domain Name System (DNS) was initiated in 1984 by John Postel and Paul Mockapetris and permitted the creation of cyberspaces. John Postel had invented the Simple Mail Transfer Protocol (SMTP) two years earlier, in 1982. Finally, in 1991, the HTML language was invented at the CERN by Tim Berners-Lee, the only core technology of the Internet not invented within the US federal system.

[60] 1985 saw the foundation of the National Science Foundation Network (NSFNET), a backbone that fulfilled the task of connecting different research centers in the United States under the TCP/IP protocol. A general understanding was also reached about how to carry out the physical expansion of the network, with governmental agencies covering the costs of the common infrastructure (Leiner, et al., 2012; Datysgeld, 2018).

[61] The opening up of the Internet to non-academic, especially commercial, uses was decided in the mid-1980s and actively prepared by the NSF. In 1992, the interconnection between the NSFNet and commercial networks was authorized, which allowed the US Government to stop funding the development of the Internet from 1993. Under a contract with NSI (now Verisign) the selling of domain names (.com, .net and .org) started to generate revenues. Currently, ICANN revenues are still linked to the selling (in fact, renting) of domain names by registrars to registrants. ICANN then funds its own operations, the management of the root system of the DNS, and subsidizes organizations

involved in the technical governance of the Internet (e.g., IETF) or those engaged in policy dialogue like the IGF or ISOC.

[62] In 1975, the IAB was established by Dave Clark and Barry Leiner. In 1986, the IETF was initiated by Mike Corrigan. The IANA was set up in 1989. Vint Cerf, Bob Kahn and Lyman Chapin founded the ISOC in 1992. The World Wide Web Consortium was established in 1993 by Tim Berners Lee, and ICANN was established in 1998.

[63] In this period of opening the Internet to the public at large and to the private sector, the federal policy was often criticized as an opaque process of privatization (Kesan & Shah, 2001), where the government was seen as favoring incumbent contractors to the detriment of competition and privileging commercial Interests (i.a. the Internet service providers and backbones operators that could exercise monopoly power) over those of citizens (privacy, security) (Mueller 1999). In addition, the legality of de facto "privatizing" public and federal resources was challenged, prompting discussion over the nature of the Internet as a public good (e.g., Froomkin, 2003)

[64] Between 1997 and 1998, ISOC attempted to bring together supporters from different stakeholder groups, as well as garner support from the United Nations and intellectual property organizations (Mueller, 2004). The US government did not give in to the pressure and refused to transfer any functions to ISOC. Jon Postel made a further attempt to challenge the government's legitimacy by staging a redirection of the DNS root to his own server, but the government forced his hand, and he was compelled to undo the move (Goldsmith and Wu, 2006). Postel passed away a few months before ICANN was founded.

[65] The loose constitution at the beginning led to many reforms without a clear mandate or a clear community of reference for accountability (Koppell, 2005). The US government and the coalition supporting ICANN (i.e., OECD governments, the business community, and the technical community once the ISOC battle was lost) managed to focus debates on questions of secondary importance: the election of a representative of "at-large members" to the ICANN Board, creation of new generic suffixes in the DNS (e.g., .kids, .xxx, .eu), and so on (see Brousseau, 2007, Brousseau et al., 2012). This "organized chaos"—according to the analysis by Jan Aart Scholte—allowed the heterarchy, a coalition of individuals claiming to represent different interest groups and a handful of US federal agencies, to retain control of the Internet expansion, architecture, and critical resources [Jan Aart Scholte, "'It's Organized Chaos': Deep Structure in Internet Governance", lecture, Sorbonne University, 2017].

[66] In the late 1980s and early 1990s, the US computer industry was in position of leadership, while European and Japanese firms led many segments of the markets in telecommunications (including TV systems) and consumer electronics. Full digitization of the IT industry rebalanced the competition in favor of the US industry.

[67] Voluntary self-regulation has strong roots in US political culture. As the United States evolved into an urban, industrial society, reformers found the concept of highly trained professionals exercising stewardship over public policy and transforming public policy issues into scientific, technical, and managerial problems more attractive than the dubious electoral politics of the 1900s. The approach emphasizes "engineering efficiency" over "inefficient" democracy and a dependence on private-sector initiatives to meet public needs, on the grounds that small groups of experts, accountable to scientific principles rather than the broad public, are more likely to arrive at effective solutions. The center of this philosophy was Herbert Hoover's "Commerce Department" (Lewis, 2010). See also Baleisen (2015) on the US tradition of expert-based regulation against the drifts of political governance (corruption, electoral politics).

[68] See, in application to several domains: Deibert (2010), Demchak and Dombrowski (2013), Gourley (2014), Zeng et al. (2017), and Stevens (2017).

[69] See, among others, Deibert and Crete-Nishihata (2012), Nocetti (2015), Zeng et al. (2017), Arsene (2018), Sieckmann and Triebel (2018), Negro (2019).

[70] China has a strong preference for the multilateral organization model, but is involved in ICANN, where it strongly defends the principle of sovereignty in various arenas. For instance, China hosted ICANN meetings in 2002 and 2013, and Chinese Internet giants such as Alibaba and Tencent, the Ministry of Industry and Information Technology, and the Internet Society of China have actively participated in ICANN's affairs in the multistakeholder model that structures the organization's activities and networks. At the same time, China and Russia have worked tirelessly in regional fora like the Shanghai Cooperation Organization and international organizations like the ITU to undermine the American position. Beyond nationalism, there is also a current of political culture against "governance without government." China, with its ambitions to become a technological superpower, has been active within the UN more broadly and the ITU specifically to shape technical standards, which would support its authoritarian vision for Internet governance. Russia is also using the ITU to advance its own technological vision, a prime example being the Digital Object Architecture (DOA), which could support Russia's "sovereign Internet." In September 2011, for example, China was

joined by other members of the Shanghai Cooperation Organization (Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan) in submitting a document titled "International Code of Conduct for Information Security" to the United Nations seeking to formalize new rules and norms in cyber governance. In 2018, a group of countries tried unsuccessfully to pass a resolution at the ITU Plenipotentiary Conference in Dubai to task an intergovernmental institution to start developing policy and regulatory guidelines for AI.

[71] See Landau (2010), Faris and Gasser (2013), Dunn Cavelty (2014), Rubinstein and Van Hoboken (2014), Andelson et al. (2015).

[72] Broeders (2015), among others, insists on the conflicting visions and cultures between members of the "technical" and "intelligence" communities. Of course, national security is oriented toward the domestic, if not the governmental, interest, whereas the security of the network as a whole is related to a broader collective interest. Though, the logic of national security also implies a much lower tolerance of risk. There is little scope for "residual risk" and "trial and error" in the realm of national security; prevention and deterrence are central to this approach. On the contrary, engineers are more pragmatic and tend to have an ex-post approach of agile responses to threats, or bugs, or identified failures. These conflicting approaches undermine cooperation.

[73] In January 2014, a large group of US cryptography and information security researchers wrote an open letter to the US government concurring with Tim Berners-Lee, stating "The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users."

[74] Laurent (2019) highlights the specific role and situation of Europe, which developed two major initiatives under the aegis of the Council of Europe: Convention 108 aimed at protecting privacy and personal data (enacted in 1981 and ratified by 47 countries in Europe (including Russia) and Latin America https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108) and the 2001 Convention on Cybercrime, dealing with the harmonization of criminal law in matters of computer-based crime and strengthening cooperation in related investigations (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185). In practice, however, Russia, Asia, Africa, and Latin America remain regions where international law cannot prevent cybercrime from occurring.

Meanwhile, the US has prioritized an approach that blurs the classic limits of what is kinetic - an essential principle for the legal regime applied to ships and planes - and what is considered as military. In the framework of NATO, they published the so-called Tallinn manual in 2013, which put forward the notion of preemptive self-defense as a legitimate principle of regulation in matters of cybersecurity; though this encountered significant resistance in that it conflicts with the Charter of the United Nations (Laurent, 2019).

The UN General Assembly created a Group of Governmental Experts (GGE), steered by the five permanent members of the UN Security Council plus Germany, tasked with drafting principles to govern cybersecurity (resolution 58/32 of December 8, 2003). However, only a limited set of recommendations were drafted after 12 years of negotiation. The ITU was unable to launch any significant initiative on the issue as the member states refused to give it a mandate.

Several cybersecurity alliances have been established at the regional level since the early 2000s. The most operational structure is the European Network and Information Security Agency (ENISA), created within the EU in 2004. The Organization of American States (OAS) initiated a Cybersecurity Program in 2004 aimed at endowing the 35 countries of North and South America with greater cybersecurity capabilities. Meanwhile, the members countries of the Shanghai Cooperation Organization (SCO) signed an Agreement on Cooperation in the Field of Information Security in 2009. Ten countries from the Association of Southeast Asian Nations (ASEAN) agreed in 2012 on a Statement on Cooperation in Ensuring Cyber Security Cooperation. All these initiatives are, however, essentially forums for exchanging good practices.

[75] Scholars list three main options for building a legal regime for cyberspace (CEIS, 2014; SFDI, 2014; Laurent 2019). First, extrapolating an existing regional legal framework such as the European one. Second, enlarging the regime applied to telecommunications (i.e., the convention founding the ITU). Third, constructing a sui generis legal regime drawing on those existing for space and sea. The three paths are very unlikely to result in successful negotiations since the first would result into an adhesion to Western principles, the second to an approach of multilateralism that is no longer supported by the West, and the third would require an agreement on the nature of cyberspace (common heritage vs. privately built shared infrastructure).

[76] The CERTs (Computer Emergency Response Teams) operationally manage cybersecurity (in a multistakeholder logic) at the national level. The CERTs' missions are to detect digital attacks on networks and to provide short term solutions, to protect the digital components of critical infrastructure (energy, transport, etc.), and to supervise the

authorities managing encryption/decryption or overseeing the routing of digital flows. They cooperate informally in networks, in practice reflecting the boundaries of diplomatic and military alliances.

[77] See Drake et al. (2016) for an exhaustive list of the origins and nature of technical, governmental, and commercial fragmentation.

[78] This view corresponds to Scholte's (2019) "sociological legitimacy," where "normative legitimacy" attached to governance arrangements meeting certain philosophically developed moral standards contrasts with "sociological legitimacy" corresponding to the acceptance and confidence - beliefs, in other words - of the subjects of a given authority in those who hold power and the system at large.

[79] In a sense, these three models also correspond to three political-economy approaches on the emergence and evolution of institutions. While generally applied to national orders, they also arguably pertain to the international one. The first model aligns with the North/Weingast/Acemoglu/Robinson approach of institutions as the results of political equilibria among dominant interest groups able to control means of violence (Hobbesian pact). Here, institutions are seen as outcomes of bargaining over the genesis and distribution of rents. The second model is more in line with the Austrian approach (Hayek/Von Mises), which considers the long-run competition among alternative institutional models and expects that the selection process will hopefully select the most efficient ones. It is also consistent with the bottom-up Jeffersonian model (vs. the top-down Hamiltonian model). The third model corresponds to the Greif/Aoki approach of institutions as equilibria based on mutually converging expectations or beliefs. In such models, institutional sponsors can play on network externalities and switching costs to trigger adhesion, while network externalities tend to stick adopters to the most widely adoption solution (see Brousseau and Raynaud, 2011).

[80] Koop (2011) highlights how (and why) accountability is relied upon to legitimate independent agencies, noting that its implementation involves incorporating all kinds of information and reporting/transparency requirements into the statutes of the organizations. This echoes the analysis of Kopell (2005), who discusses the various dimensions of accountability - such as transparency, liability, controllability (whether the organization acts in conformity with its mission), responsibility (whether the organization follows the rules) - and why it was complex for an organization like ICANN to meet contradictory expectations from various stakeholders, which undermined its design and effectiveness.

References

Abbate, Janet. *Inventing the Internet*. Cambridge, MA and London: MIT Press, 1999.

Abelson Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J. Weitzner, "Keys under doormats: mandating insecurity by requiring government access to all data and communications", *Journal of Cybersecurity*, 1, No 1, (2015), 69–79,

Aguiton, Christophe and Dominique Cardon. "The coordination of international civil society and uses of the internet" in in *Governance, Regulations, Powers on the Internet*, Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds), Cambridge: Cambridge University Press, (2012), 275-294

Arsène, Séverine. "China, Internet Governance and the Global Public Interest." In *A New Responsible Power China? China's Public Diplomacy for Global Public Goods*, Ines Sieckmann and Odila Triebel (eds.), 68-77. Stuttgart, D.: ifa Edition Culture and Foreign Policy, 2018.

Balbi, Gabriele and Andreas Fickers (eds), History of the International Telecommunication Union (ITU); Transnational techno-diplomacy from the telegraph to the Internet, Oldenburg: De Gruyter, 2020

Balleisen, Edward. J. "The Dialectics of Modern Regulatory Governance", in *Business Regulation, volume 1; The Invention of the Modern Regulatory State*, Edward J. Balleisen (ed), Cheltenham: Edward Elgar, xvii-xcvii (2015)

Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. 1996. https://www.eff.org/cyberspace-independence.

Besen, Stanley M., and Joseph Farrell. "The role of the ITU in Standardization: Pre-eminence, impotence or rubber stamp?" *Telecommunications Policy* 15, no. 4 (1991): 311-321.

Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward Strategy for Cyber-Power*. Abingdon, Oxfordshire: Routledge for the International Institute for Strategic Studies, 2011.

Bovens, Mark. "New Forms of Accountability and EU-Governance." *Comparative European Politics* 5, no. 1 (2007): 104–120.

Braithwaite John and Peter Drahos, *Global Business Regulation*. Cambridge: Cambridge University Press, 2000

Broeders, Dennis. *The public core of the Internet, an international agenda for Internet Governance*. Amsterdam University Press: Amsterdam, 2015.

Bronckers, Marco, and, Pierre Larouche. "A Review of The WTO Regime For Telecommunications Services." In *The World Trade Organizations and Trade in Services*, edited by M. Andenas and K. Alexander, 3315-375. Brill NV, The Netherlands, 2007.

Brousseau, Eric and Emmanuel Raynaud "Climbing the Hierarchical Ladders of Rules": A Life-cycle Theory of Institutional Evolution", *Journal of Economic Behavior and Organization*, 79, pp. 65–79, (2011)

Brousseau, Eric and Meryem Marzouki. "Internet Governance: Old Issues, New Framings, Uncertain Implications" in *Governance, Regulations, Powers on the Internet*, Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds), Cambridge: Cambridge University Press, (2012), 368-397.

Brousseau, Eric and Thierry Pénard. "The Economics of Digital Business Models: A Framework for Analyzing the Economics of Platforms", *Review of Network Economics*, 6, n°2, (2007). 81-114

Brousseau, Eric, and Meryem Marzouki. "Internet governance: old issues, new framings, uncertain implications." In *Governance, Regulation and Powers on the Internet,* Brousseau Eric, Marzouki Meryem, and Méadel Cécile. Cambridge: Cambridge University Press, 2012

Brousseau, Eric, Jérôme Sgard and Yves Schemeil. "Delegation without borders: On individual rights, constitutions and the global order", *Global Constitutionalism*, 1, No 3, (2012) 455 484

Brousseau, Eric, Meryem Marzouki and Cécile Méadel (eds.). *Governance, Regulations, Powers on the Internet*, Cambridge Cambridge University Press, 2012

Brousseau, Eric. "Public and Private Governance of the Digital Space: Does a second rank Institutional Framework exist?", in *Internet and Digital Economics, Theories and Applications*, Eric Brousseau and Nicolas Curien (eds), Cambridge: Cambridge University Press, 2007. 617-648,

Cammaerts, B. "Multi-Stakeholderism and Intra-Civil Society Networking: The case of The WSIS IG-working group mailing list and its aftermath in The Handbook on Global Media and Communication Policy, Robin E. Ansell and Mark Raboy (eds), Oxford: Wiley-Blackwell, (2011), 131-146

Cammaerts, Bart, "*Disruptive sharing in a digital age: rejecting neoliberalism?" Continuum: Journal of Media and Cultural Studies*, 25 (1). (2011) pp. 47-62

Cammaerts, Bart, and Nico Carpentier. "The Unbearable Lightness of Full Participation in a Global Context: WSIS and Civil Society Participation." In *Towards a Sustainable Internet Society: Deconstructing WSIS* Servaes J, Carpentier N (eds), 17–49. Intellect Books: Bristol, UK, 2006.

Carpenter, Brian E. *Network Geeks: How They Built the Internet*. New York: Copernicus, 2013

Carr, Madeline. "Power Plays in Global Internet Governance". *Millennium: Journal of International Studies* 43, no. 2 (2015): 640–659.

CEIS. *Les droits maritimes et de l'espace peuvent-ils inspirer un droit du cyberespace ?*. Paris, CEIS, 2014, 66 p

Cerf, Vinton G. (Chair) et al., "ICANN's Role in the Internet Governance Ecosystem." Report of the ICANN Strategy Panel, February 20, 2014.

Chenou, Jean-Marie and Roxana Radu. "Relationship between Internet organizations and IGOs: beyond turf wars." Paper presented at the 23d World Congress of Political Science, Montréal, July 2014.

Chenou, Jean-Marie. "Is Internet Governance a Democratic Process? Multistakeholderism and Transnational Elites." paper, ECPR Conference, 2011.

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA.: MIT Press, 2012.

Christou, George, and Seamus Simpson. "The New Electronic Marketplace: European Governance Strategies." In *a Globalising Economy*, 75-87. Cheltenham: Edward Elgar Pub, 2007.

Clinton, William, and Albert Gore. *Framework for e-commerce*. Washington, DC: White House, 1996.

Codding, George A, and Anthony M. Rutkowski. *The International Telecommunication Union in a changing world*. Dedham, MA: Artech House, 1982.

Codding, George A. "Evolution of the ITU." T*elecommunications Policy* 15, no. 4 (1991): 271-285.

Cohen, Julie E. *Between Truth and Power: Legal Constructions of Informational Capitalism*. New York: Oxford University Press, 2019.

Collar, Emilio, and Roy J. Girasa. "Who Governs the Internet? International Legal Aspects of IT Governance." *The Business Review, Cambridge* 16, no. 2 (2010): 1-15.

Cornish, Paul. "Governing Cyberspace through Constructive Ambiguity." *Survival* 57, no. 3 (2015): 153-176.

Cowhey, Peter, and Jonathan D. Aronson. "The ITU in transition." *Telecommunications Policy* 15, no. 4 (1991): 298-310.

Cox, Robert, and Harold K. Jacobson. *The Anatomy of Influence: Decision Making in International Organization*. New Haven (Conn.): Yale University Press, 1973.

Datysgeld, Mark W. "Understanding the role of States in Global Internet Governance: ICANN and the question of legitimacy." XII Annual Giganet Symposium, December 2017, Geneva, Final paper published in August (2018)

David, Paul. "Clio and the Economics of QWERTY", *American Economic Review*, 75, N°2, (1985), 332-337

De Moor, Tine. "Three Waves of Cooperation: A Millennium of Institutions for Collective Action in Historical Perspective", in *The Oxford Handbook of Institutions of International Economic Governance and Market Regulation*, Eric Brousseau, Jean-Michel Glachant, Jérôme Sgard (eds.), Oxford : Oxford University Press, (2022)

De Nardis, Laura. *The global war for internet governance*. New Haven: Yale University Press, 2014.

de Vey Mestdagh, Kees (C. N. J.), & Rijgersberg, Rudolf W. Internet Governance and Global Self Regulation: Building Blocks for a General Theory of Self Regulation. *Legisprudence: International Journal for the Study of Legislation*, *4*(3), (2010). 385 - 404.

Deibert, Ronald J. "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace." In *Routledge Handbook of Internet Politics*, edited by Andrew Chadwick and Philip N. Howard, 323-336. London: Routledge, 2010.

Deibert, Ronald J., "Bounding cyber power: escalation and restrain in global cyberspace." The Centre for International Governance Innovation. Internet Governance Papers: Paper No. 6, (2013). https://www.cigionline.org/sites/default/files/no6_2.pdf

Deibert, Ronald J., and Masashi Crete-Nishihata. "Global Governance and the Spread of Cyberspace Controls." *Global Governance* 18, no. 3 (2012): 339-361.

Demchak, Chris, and Peter Dombrowski. "Cyber Westphalia: Asserting State Prerogatives in Cyberspace." Georgetown Journal of International Affairs, Special Issue, (2013), 29-38

DeNardis, Laura, and Francesca Musiani, "Governance by Infrastructure." In *The Turn to Infrastructure in Internet Governance*, Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson (eds). New York: PalgraveMacmillan, 2016.

Denardis, Laura, and Mark Raymond. "Thinking Clearly about Multistakeholder Internet Governance." *Eighth Annual GigaNet Symposium*. Bali, 2013.

DeNardis, Laura. *The Global War for Internet Governance*. New Haven, CT: Yale University Press, 2014.

Dingwerth, Klaus. "From international politics to global governance? The case of nature conservation (Garnet Working Paper No. 46(8))." Institute for Intercultural and International Studies, University of Bremen, 2008.
http://www2.warwick.ac.uk/fac/soc/pais/research/researchcentres/csgr/garnet/workingpapers/4608.pdf

Drake, William J, Vinton G. Cerf, and Wolfgang Kleinwächter. "Internet Fragmentation: An Overview." Future of the Internet Initiative White Paper, World Economic Forum, January 2016.

Drezner, Daniel W. "The Global Governance of the Internet: Bringing the State Back In." *Political Science Quarterly* 119, no. 3 (2004): 477-498.

Dunn Cavelty, Myriam. "Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20, no. 3 (2014): 701-715.

Elkin-Koren Niva, and Maayan Perel. "Understanding Algorithmic Governance in a Digital Era", in *The Oxford Handbook of Institutions of International Economic Governance and Market Regulation*, Eric Brousseau, Jean-Michel Glachant, Jérôme Sgard (eds.), Oxford : Oxford University Press, (2022)

Epstein, Dmitry. "The making of institutions of information governance: the case of the Internet Governance Forum." *Journal of Information Technology* 28, no. 2 (2013): 137–149.

Farina, Cynthia R., Dmitry Epstein, Josiah Heidt, and Mary J Newhart. "Designing an online civic engagement platform: Balancing "more" vs. "better" participation in complex public policymaking." *International Journal of E-Politics* 5, no. 1 (2014): 16– 40

Faris, Robert, and Urs Gasser. "Governments as Actors." In *Internet monitor 2013: Reflections on the Digital World*, U. Gasser, R. Faris and R. Heacock (eds.), 19-24. Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University, 2013.

Fontaine-Skronski, Kim, and Michele Rioux. "Conceptualising institutional changes in a world of great transformations - From the Old telecommunications regime to the new Global Internet Governance." In *Global Governance Facing Structural Changes New Institutional Trajectories for Digital and Transnational Capitalism* edited by Kim Fontaine-Skronski and Michèle Rioux, (Eds.), 59-78. Palgrave Macmillan, 2015.

Froomkin, Michael A. "Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace." *Harvard Law Review* 116, no. 3 (2003): 749–873.

Glen, Carol M. "Internet governance: Territorializing cyberspace?" *Politics & Policy* 42, no. 5 (2014): 635-57.

Goldsmith, Jack and Timothy S. Wu, *Who Controls the Internet?: Illusions of a Borderless World.* Oxford: Oxford University Press, 2006.

Gourley, Stephen K. "Cyber Sovereignty." In *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther. Boca Raton, 277-290. FL: Taylor and Francis, (2014)

Greif, Avner, and Jared Rubin, "Endogenous Political Legitimacy: The English Reformation and the Institutional Foundations of Limited Government", Working Paper Stanford University, September 2015

Heath, Don. "Beginnings: internet self-governance: a requirement to fulfill the promise." ITU, 1997. http://www.itu.int/newsarchive/projects/dnsmeet/ HeathAddress.html

Herrmann-Pillath, Carsten. "Ways out of the globalization trilemma: Deliberating trade policy", in *The Oxford Handbook of Institutions of International Economic Governance and Market*

Regulation, Eric Brousseau, Jean-Michel Glachant, Jérôme Sgard (eds.), Oxford: Oxford University Press, (2022)

Hill, Richard. "Internet Governance, Multi-Stakeholder Models, and the IANA Transition: Shining Example or Dark Side?" *Journal of Cyber Policy* 1, (2016): 176-197.

Hooghe, Liesbet, Tobias Lenz, and Gary Marks. A Theory of International Organization. Oxford: Oxford University Press (2019)

ISOC. "Internet Ecosystem: Naming and addressing, shared global services and operations, and open standards development." Working Paper, Internet Society, Geneva, Feb. 2014. https://www.internetsociety.org/internet/who-makes-it-work

ITU (2011) The ITU Council., Available from URL: http://www.itu.int/council/index.html.

ITU (International Telecommunication Union) (1994) Convention of the International Telecommunication Union, Art. 19. Available from URL: http://www.itu.int/net/about/basic-texts/constitution/chapteri.aspx.

ITU, "The missing link: report of the Independent Commission for World-Wide Telecommunications Development", ITU/Document # 6302, Geneva : ITU, (1984)

ITU, *From Semaphore to Satellite*, Geneva: ITU, (1965)

Jayawardane, Saah, Joris Larik, and Erin Jackson. "Cyber governance: challenges, solutions and lessons for effective global governance" Policy Brief 17, The Hague Institute for Global Justice. 2015. https://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf

Kahler, Miles, and David Lake. "Economic Integration and Global Governance: Why So Little Supranationalism?" in *The Politics of Global Regulation*, eds Walter Mattli and Ngaire Woods Princeton, NJ: Princeton University Press, 2009.

Katz, Michael L. and Carl Shapiro. "Network Externalities, Competition, and Compatibility", *American Economic Review*,75, No. 3, (1985), 424-440

Kesan, Jay P., and Rajiv C. Shah. "Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System." *Washington University Law Review 79, no. 1* (2001)

Klein, Hans, and Milton Mueller. "What to Do About ICANN: A Proposal for Structural Reform." Concept Paper, the Internet Governance Project, 2005.

Klein, Hans. "ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy." *The Information Society* 18, no. 3 (2002) :193–207.

Kleinwächter, Wolfgang, "Multistakeholderism, Civil Society, and Global Diplomacy: The Case of the World Summit on the Information Society", in William J. Drake and Ernest J. Wilson III, Governing Global Electronic Networks: International Perspectives on Policy and Power, Boston: MIT Press, 2008

Kleinwaechter, Wolfgang. "Beyond ICANN vs. ITU? How WSIS tires to enter the new territory of Internet governance." *Gazette* 66, no. 3-4 (2004): 233 - 251.

Koop, Christel. "Explaining the Accountability of Independent Agencies: The Importance of Political Salience." *Journal of Public Policy* 31, no. 2 (2011): 209–234.

Koppell, Jonathan G S. "Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"." *Public Administration Review* 65, no. 1 (2005): 94-108.

Kruger, Lennard G. "Internet Governance and the Domain Name System: Issues for Congress." Congressional Research Service Report, Washington DC. 7-5700, R42351, November 2014. https://crsreports.congress.gov/product/pdf/R/R42351

Kruger, Lennard G. "The future of Internet governance: should the United States relinquish its authority over ICANN?" Congressional Research Service Report. 1 September 2016. R44022, https://www.fas.org/sgp/crs/misc/R44022.pdf

Kurbalija, Jovan. *An Introduction to Internet Governance 7th Edition*. Msida: DiploFoundation, 2016.

Kwalwasser, Harold. "Internet Governance." In. *Cyberpower and National Security,* Kramer, Franklin, Stuart Starr, Larry Wentz, chap 21. Washington: Center for Technology & National Security Policy, 2009.

Landau, Susan. *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, Cambridge (Mass.): MIT Press, 2010.

Laurent, Sébastien-Yves. "Les gouvernances mondiales fragmentées de l'Internet." Working Paper, Institut de Recherche Montesquieu, Université de Bordeaux, September 2019.

Lee, Kelley. *Global telecommunications regulation: a political economy perspective*. United Kingdom: Lincoln, 1995.

Leiner, Barry M. *Brief History of the Internet.* Internet Society, 2012. https://www.internetsociety.org/internet/history-internet/brief-history-internet/

Lessig, Lawrence. *Code, and other laws of cyberspace*. New York, NY: Basic Books, 1999.

Levinson, Nanette S, and Meryem Marzouki. "International Organizations and Global Internet Governance: Interorganizational Architecture." In *The Turn to Infrastructure in Internet Governance*, Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson (eds), 47-72. New York: Palgrave Macmillan, 2016.

Lewis, James A. "Sovereignty and the Role of Government in Cyberspace." *Brown Journal of World Affairs* 16, no. 2 (2010): 55-65.

Liaropoulos, Andrew N. "Cyberspace Governance and State Sovereignty." In *Democracy and an Open-Economy World Order* edited by George C. Bitros and Nicholas C. Kyriazis, 25-36. Cham, Switzerland, 2017.

Liaropoulos, Andrew. "Reconceptualising cyber security: Safeguarding human rights in the era of cyber surveillance." *International Journal of Cyber Warfare and Terrorism* 6, (2016): 33–41.

Liebowitz, S. J. and Stephen E. Margolis, "Path Dependence, Lock-in, and History", *Journal of Law, Economics, & Organization*, 11, No. 1 (1995), 205-226

Liu, Han-Wei. "International Standards in Flux: A Balkanized ICT Standard-Setting Paradigm and its Implications for the WTO." *Journal of International Economic Law* 17, no. 3 (2014): 551–600

Lyall, Francis. *International Communications: The International Telecommunication Union and the Universal Postal Union*. Farnham, UK: Ashgate Publishing, 2011.

Malcolm, Jeremy, "Oversight Transition Isn't Giving Away the Internet, But Won't Fix ICANN's Problems", Electronic Frontier Foundation, October 3, 2016, https://www.eff.org/deeplinks/2016/09/oversight-transition-isnt-giving-away-internet-wont-fix-icanns-problems

Malcolm, Jeremy, Criteria of meaningful stakeholder inclusion in internet governance. *Internet Policy Review*, *4*(4). (2015).

Marsden, Christopher, *Regulating the Global Information Society,* Routledge, 2005

Marsden, Christopher. *Net Neutrality: Towards A Co-Regulatory Solution*, Bloomsbury Publishing, 2010

Mathiason, John. *Internet Governance. The New Frontier of Global Institutions*. New York: Routledge, 2009.

McEvoy Manjikian, Mary. "From global village to virtual battlespace: the colonizing of the Internet and the extension of realpolitik." *International Studies Quarterly* 54, no. 2 (2010): 381- 401.

Meyer, Victor. *L'Union Internationale des Telecommunications et Son Bureau*, ITU, Geneva, 1946

Morten Haugen, Hans. "The crucial and contested global public good: principles and goals in global internet governance." *Internet Policy Review* 9, no. 1 (2020)

Mueller, Milton L. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: MIT Press, 2004.

Mueller, Milton, and Ben Wagner. "Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance." Center for Global Communication Studies, Annenberg School for

Communication, 2014.
https://www.internetgovernance.org/wp-content/uploads/MiltonBenWPdraft_Final_clean2.pdf

Mueller, Milton, and Brenden Kuerbis. "Towards Global Internet Governance: How To End U.S. Control of ICANN Without Sacrificing Stability, Freedom or Accountability" tprc Conference Paper, 2014.

Mueller, Milton. "Critical resource: An institutional economics of the Internet addressing-routing space." *Telecommunications Policy* 34, no. 8 (2010): 405–416.

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

Negro, Gianluigi. "A history of Chinese global Internet governance and its relations with ITU and ICANN." *Chinese Journal of Communication* 13, no. 25 (2019): 1-18.

Nocetti, Julien. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91, no. 1 (2015): 111-130.

Nonnecke, Brandie Martin, and Dmitry Epstein. "Crowdsourcing Internet Governance: The Case of ICANN's Strategy Panel on Multistakeholder Innovation." GigaNet: Global Internet Governance Academic Network, Annual Symposium, 2016.
http://dx.doi.org/10.2139/ssrn.2909353_

Nye, Joseph S. JR. "The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series 1". Waterloo, ON: Global Commission on Internet Governance, 2014. https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/

Nye, Joseph. S, and John D.Donahue. *Governance in a globalizing world*. Washington, DC: Brookings Institution Press, 2010.

Parker, Geoffrey, Georgios Petropoulos, and Marshall Van Alstyne. "Digital Platforms and Antitrust", in *The Oxford Handbook of Institutions of International Economic Governance and Market Regulation*, Eric Brousseau, Jean-Michel Glachant, Jérôme Sgard (eds.), Oxford : Oxford University Press, (2022)

Pelkey, James, *Entrepreneurial Capitalism and Innovation: A History of Computer Communications 1968-1988*, nov 2007.
http://www.historyofcomputercommunications.info/index.html.

Raboy, Marc, and Normand Landry. *Civil Society, Communication and Global Governance: Issues from the World Summit on the Information Society*. New York: Peter Lang Academic Publishing, 2005

Raboy, Marc, Normand Landry and Jeremy Shtern. *Digital Solidarities, Communication Policy and Multi-stakeholder Global Governance: The Legacy of the World Summit on the Information Society*. New York: Peter Lang Academic Publishing, 2010.

Radu, Roxana. *Negotiating internet governance*. Oxford: Oxford University Press, 2019.

Raustiala, Kal. "An Internet Whole and Free: Why Washington was right to give up control." *Foreign affairs* 96, no. 140 (2017): 140-147.

Raymond, Eric Steven. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. O'Reilly Media.1999.
http://www.catb.org/~esr/writings/cathedral-bazaarr

Richardson, Alan J., and Burkard Eberlein. "Legitimating Transnational Standard- Setting: The Case of the International Accounting Standards Board." *Journal of Business Ethics,* no. 98 (2011): 217–245.

Rochet, Jean-Charles and Jean Tirole, "Platform Competition in Two-sided Markets", *Journal of the European Economic Association*, 1, No. 4 (2003), 990-1029

Rogers, Kevin M. "The Early Ground Offensives in Internet Governance." *International Review of Law Computers & Technology* 21, No. 1 (2007): 5–14.

Rosenau, James N. "Governance in the twenty-first century." *Global Governance* 1, no. 1 (1995): 13-43.

Rosenau, James N., and Ernst-Otto Czempiel. *Governance without government: order and change in the world politics*. Cambridge: Cambridge University Press, 1992.

Rotenberg, Marc. "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)." *Stanford Technology Law Review* 1 (February 2001).
http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf.

Rubinstein, Ira and van Hoboken, Joris V. J., "Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era" *Maine Law Review* 488 (2014), NYU School of Law, Public Law Research Paper No. 14-46

Rutkowski, Anthony M. "The ITU at the cusp of Change" *Telecommunications Policy August* 15, no.4 (1991): 286-297.

Ryan, Patrick S. "The ITU and the Internet's Titanic Moment." *Stanford Technology Law Review*. no. 8 (2012): 1-36.

Saltzer, Jerome, David Reed, and David Clark. "End-to-end Arguments in System Design." *ACM Transactions on Computer Systems* 2, no. 2 (1984): 277-288.

Savage, James G. *The Politics of International Telecommunications Regulation*. Westview Press, 1989.

Schemeil, Yves. "Global governance: evolution and innovation in international relations." In *Regulation and Powers on the Internet*, Brousseau Eric, Marzouki Meryem, and Méadel Cécile Governance, 186-208. Cambridge: Cambridge University Press, 2012.

Scholte, Jan Aart. "Polycentrism and Democracy in Internet Governance." In *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance* U. Kohl (ed.), 165-184. Cambridge: Cambridge University Press, 2017.

Scholte, Jan Aart. "Sources of Legitimacy in Global Governance." *Outlines of Global Transformations: Politics, Economics, Law* 12, no. 3 (2019): 47–76.

Shen, Yi. "Cyber sovereignty and the governance of global cyberspace." *Chinese Political Science Review* 1 no. 1 (2016): 81-93.

Sieckmann, Ines and Odila Triebel, *A New Responsible Power China? China's Public Diplomacy for Global Public Goods,* Institut für Auslandsbeziehungen, IFA Edition Culture and Foreign Policy (2018)

Slotten, Hugh Richard. "The International Telecommunications Union, Space Radio Communications, and U.S. Cold War Diplomacy, 1957-1963." *Diplomatic History* 37, no. 2 (2013): 313-371.

Snyder, Joel, Konstantinos Komaitis, and Andrei Robachevsky. "The History of IANA: An Extended Timeline with Citations and Commentary." 2017. https://www.yumpu.com/en/document/view/56851186/the-history-of-ianaan-extended-timeline-with-citations-and-commentary/12.

Stevens, Tim, "Cyberweapons: power and the governance of the invisible". *International Politics,* 55, (2018) 482–502

Take, Ingo. "Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS." *Regulation & Governance* 6, no. 4 (2012): 499–523.

Tallberg, Jonas, Thomas Sommerer, Theresa Squatrito and Christer Jönsson, "Explaining the Transnational Design of International Organizations", International Organization, 68, No. 4 (2014), 741-774

Tallberg, Jonas, Karin Backstrand, and Jan Aart Scholte. *Legitimacy in Global Governance: Sources, Processes, and Consequences*. Oxford: Oxford University Press, 2018.

Tallberg, Jonas, Thomas Sommerer, Theresa Squatrito and Christer Jönsson. "Explaining the Transnational Design of International Organizations". *International Organization* 68(4): 741-774, 2014 [with].

Taylor, Emily. "ICANN: Bridging the Trust Gap (Global Commission on Internet Goverance: Paper Series: no. 9)." London UK: Centre for International Governance Innovation and Chatham House, march 2015.

Teleanu, Sorina. "The IANA stewardship transition: what is happening? (Part I)." Diplo, 2016. https://www.diplomacy.edu/blog/iana-stewardship-transition-what-happening-part-i

Townes, Miles. "The Spread of TCP/IP: How the Internet Became the Internet." *Millennium - Journal of International Studies* 41, no. 1 (2012): 43- 64.

UN WGIG (United Nations Working Group on Internet Governance). *Report of the Working Group on Internet Governance* [Report]. 2005, www.wgig.org/docs/WGIGREPORT.pdf

UN WSIS (United Nations World Summit on the Information Society). *Declaration of Principles, A/C.2/59/3*, 2003.

Vincent, Charles, and Jean Camp. "Looking to the Internet for models of governance." *Ethics and Information Technology,* no.6 (2004): 161–173.

Von Bernstorff, Jochen. "Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony." *European Law Journal* 9, no. 4 (2003): 511 - 526.

Weimer, David L. "The Puzzle of Private Rulemaking: Expertise, Flexibility, and Blame Avoidance in U.S. Regulation." *Public Administration Review* 66, no. 4 (2006): 569-582.

Weiss, Thomas G., and Rorden Wilkinson. *International Organization and Global Governance*. Abingdon: Routledge, 2018.

Weiss, Thomas G., Tatiana Carayannis, and Richard Jolly, "The "Third" United Nations", *Global Governance,* 15, no 1, (2009), 123–142

West, Sarah. "Globalizing Internet governance: Negotiating cyberspace agreements in the post-Snowden era." Conference Paper, TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy, 2014.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418762

Winn, Jane, "Globalization and Standards: The Logic of Two-Level Games", *I/S: Journal of Law and Policy for the Information Society*, 5, No 2 (2009), 185-218

Woodrow, R. Brian. "Tilting towards a trade regime The ITU and the Uruguay Round services negotiations." *Telecommunications Policy* 15, no. 4 (1991): 323-342.

Wu, Timothy S. "Cyberspace Sovereignty? The Internet and the International System." *Harvard Journal of Law and Technology* 10, no. 3 (1997): 647-666.

Wu, Timothy S. "When Code Isn't Law". *Virginia Law Review* 4 (2003b): 671-751.

Ypsilanti, Dimitri. "Book review of Lyall's 'International Communications: The International Telecommunication Union and the Universal Postal Union'." *Telecommunications Policy* 37, no. 11 (2013): 1168–1169.

Zalnieriute, Monika. "From Human Rights Aspirations to Enforceable Obligations by Nonstate Actors In The Digital Age: The Case Of Internet Governance And ICANN." *Yale Journal of Law & Technology* 21, no. 1 (2019): 278-336

Zeng, Jingha, Stevens Tim, and Chen Yaru. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"." *Politics & Policy* 45, no. 3 (2017): 432-464.

Chaire Gouvernance et Régulation
Fondation Paris-Dauphine
Place du Maréchal de Lattre de Tassigny - 75016 Paris (France)
http://chairgovreg.fondation-dauphine.fr