Understanding the role of States in Global Internet Governance: ICANN and the question of legitimacy

Mark W. Datysgeld, Master in International Relations, São Paulo State University

[www.markwd.website]

Summary

"For all the breathless talk of the supreme placelessness of our new digital age, when you pull back the curtain, the networks of the Internet are as fixed in real, physical places as any railroad or telephone system ever was."

(Andrew Blum)

Abstract

The term "global governance" gained renewed significance with the expansion of the Internet Governance regime, an arrangement in which most institutions make use of the multistakeholder model to generate norms, with spaces for open dialogue and decision-making that includes most interested actors. This presents a deviation from the model traditionally studied by global governance, which is that of the United Nations and its multitude of agencies, where despite the inclusion of other actors, most of the time States are still at the focal point of the norm-setting process. With a focus on the Internet Corporation for Assigned Names and Numbers (ICANN), the main objective of this study is that of understanding where the legitimacy of the actors involved in leading this regime comes from, and in order to do that, we: A) examine the formation of the DNS per se and why it provides a measure of power to the actor that controls it; B) evaluate how legitimacy was established by the actors who took on leading positions within the Internet Governance regime; and C) understand how subsequently the dynamics between State and private actors in this multistakeholder environment were consolidated. We use Weber's "Three Types of Legitimate Rule" to analyze power dynamics within the model, and conclude that a great deal of power was held by the academics who built the network, and as it became larger and more consolidated, private and government actors have made significant efforts to gain increased control over it, with some degree of success.

Keywords: Global Governance, ICANN, Internet Governance, Legitimacy, Multistakeholder process

Contextualization and Disclaimer

This paper is the result of research carried out over the course of approximately three years by Mark W. Datysgeld, with the goal of obtaining an International Relations master's degree at the Graduate Program in International Relations San Tiago Dantas, a joint initiative of the São Paulo State University (UNESP), the University of Campinas (UNICAMP), and the Pontifical Catholic University of São Paulo (PUC-SP). The thesis was defended and accepted on May 10, 2017 by a panel consisting of Dr. Carlos Gustavo Poggio Teixeira, Dr. Lucas da Silva Tasquetto, and Dr. Flávia de Campos Mello. One year of this research was funded by the Brazilian Federal Agency for Support and Assessment of Post-graduate Education (CAPES).

Apart from empirical methods, extensive field research and interviewing was also carried out. The thesis incorporates as an appendix interviews with the following people of interest: Dr. Olga Cavalli (then GAC's Vice-chair, representing Argentina), Manal Ismail (current GAC Chair, representing Egypt), Pedro Ivo da Silva (Brazilian GAC), Jaifa Mezher Arango (Colombian GAC), Jose Raúl Solares Chiu (Guatemalan GAC), Vanda Scartezini (former ICANN Board and Brazilian GAC), Kathryn Kleinman (NCUC co-founder), Yannis Li (Executive director for .asia), Maxim Alzoba (Operator for .moscow), Martin Silva Valent (GNSO Council), Hamza Ben Mehrez (former Hivos/DiploFoundation consultant), Lucky Masilela (AFRINIC Board), as well as Megan Richards and Cristina Monti (European Commission).

Field research includes ICANN meetings number 53 in Buenos Aires, 55 in Marrakesh, 56 in Helsinki, 58 in Copenhagen, 59 in Johannesburg, 60 in Abu Dhabi, and 61 in San Juan; IGFs number 10 in João Pessoa, 11 in Guadalajara, and 12 in Geneva; LACIGF number 9 in Costa Rica; the South School of Internet Governance and the Brazilian School of Internet Governance; as well as local events organized by ISOC, the Brazilian Association of Internet and Telecommunications Providers (ABRINT), and NIC.br.

The budget for some of the ICANN meetings was partially covered by the institution, by means of their NextGen and Fellowship outreach programs, which are open to the global community and make it possible for interested parties to access their assemblies and learn more about the policymaking process. There is no commitment, explicit or implicit, between the researcher and the institution that affects in any manner the contents of this paper. The budget for João Pessoa's IGF was provided by NIC.br, while budget for Geneva's IGF was partially provided by ICANN'S Business Constituency, and LACIGF funding was partially provided by ISOC. Travel budget for the South School of Internet Governance was provided by Dominios Latinoamérica, while budget for the Brazilian School of Internet Governance was provided by NIC.br.

1. Introduction: The consolidation of Internet Governance

The purpose of this article is to analyze how the structures of power within Internet Governance were formed, with particular effort placed on understanding the role of States in an arrangement where they are not the leading actor, but rather a participant with a similar role to that of remaining stakeholders. It is our understanding that to do so, it is necessary to explore the nature of the power packaged within the Internet Governance label, what qualifies leading stakeholders as legitimate, and observe how this digital space was seized from a historical perspective.

This depth of analysis is necessary because the almost ad-hoc manner in which the Internet was developed over the past few decades ended up shaping a regime[1] that at a glance seems quite unique in comparison to others that operate at a global level. At first led by academics doing research on governmental funds and then being moved forward with the cooperation of the private sector, this arrangement is one of the drivers of the multistakeholder model, presenting an environment that is fairly open to the participation of any interested party and accumulating some triumphs over its existence.

Delimiting the initial role of governments as that of sponsors of the regime is not an exaggeration, but rather a consequence of the approach taken by States towards the Internet. The burden of developing the technology and setting its standards was shared mostly between universities of the United States in the shaping of the military-backed ARPANET. A smaller contingent of researchers from Europe worked on networks such as CYCLADES, which was financed by the French government (HAFNER and LYON, 1998).

Eventually, the viability of internetworking as a platform for early commercial purposes started to present itself, and businesses proceeded to make more significant investments in developing their networking solutions, in parallel to the efforts carried out by the academic sector. Meanwhile, heavy development of networks by governments could be observed mainly in the United States, where there was a growing interest by different internal agencies to integrate the technology into their workflow (LEINER, CERF, *et al.*, 2012).

The primary assembly of the network of networks by and large took place between North America and Western Europe, repeating the pattern that had been observed during the expansion of the telegraphic grid in the 19th century, whose cables would eventually be key in enabling the nearly global reach of telephony, and in consequence those same cables would act as the foundation of the transoceanic connections that form the Internet. The early technological dominance established by

---

[1] Regime here is used in its International Relations interpretation, defined as a set of explicit or implicit principles, norms, rules, and decision making procedures around which actor expectations converge in a given issue-area (KRASNER, 1983).

these States remained and still remains relevant to understanding how power structures were formed in regards to global communications systems (STANDAGE, 2014).

In this sense, early norms affecting the Internet were set by a group of academics from the Global North who apprehended technical aspects of the network, finding themselves more or less on equal footing as they collectively developed this new means of communication. A possible exception to this rule was Jon Postel, accepted by most as an informal mediator of that epistemic community due to his technical capacity and eloquence, rather than due to the formal position held by him; later in life he would famously move on to maintain the first root name server (HAFNER and LYON, 1998).

Born out of a 1969 meeting between pioneers Crocker, Carr and Rulifson, the chosen method for proposing standards for the network was the "Request for Comments", or RFC. These documents were not made up of recommendations set in stone, but rather illustrated how and why conclusions were reached, inviting interested parties to pitch in and work on top of the proposal, or to just outright refuse them if a convincing enough argument for that could be made (PELKEY, 2007).

This rendered the norm-setting process more transparent and collaborative, eventually growing into a tradition that carried over into the Internet Engineering Task Force (IETF), as well as informing the communal ideology behind the Internet Governance regime as a whole. Let this not be taken as evidence of an early multistakeholder approach, though, as the majority of actors involved were more or less formally contracted by the United States government.

These ideals that valued mutual aid and a sense of collectivity between the youth who around the late 1960s were shaping the nascent computer industry should come as no surprise, seeing as they were immersed in an environment where counterculture movements were at their height, and concepts such as a desire for the end of wars, increased personal liberties, and the hippie movement as a whole were quite widespread in the occident (MARKOFF, 2005).

The concept of modeling the network into an "open, minimalist, and neutral" space was consolidated during this era, and eventually this became one of the factors that informed the United States military's decision to fork into its own network, leaving the ARPANET's fortune largely to the academics. Internetworking with an increasing number of universities followed, eventually more or less forcing from the bottom-up the whole network into the Internet Protocol Suite (TCP/IP), in lieu of the top-down Open Systems Interconnection (OSI) that was championed by the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO), who could be seen as more legitimate under a traditional perception of global governance (WU, 2008).

As the Internet began to consolidate, its main infrastructure was still controlled by the United States government, as was the Domain Name System (DNS) and the IANA functions that coordinate the root of the names and numbers on the network. Years of warring over the control of Internet Governance by various groups and stakeholders followed, particularly advanced by a group of pioneers that huddled around the nascent Internet Society (ISOC). However, in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was formed in response to a request by the Clinton administration to transition the DNS from a liability to the United States government into an asset led by the private sector that would allow for international input into its policies, but still remain under supervision of the United States (MUELLER, 2004).

ICANN was granted stewardship over the IANA functions, and put under the obligation of creating and regulating competition within the domain names market, while at the same time managing a disputes resolution process that had dynamics suited for the rapid pace of the Internet. Following a series of recommendations by the World Intellectual Property Organization (WIPO), a mandatory process built into domain name contracts named Universal Dispute Resolution Policy (UDRP) was established to address such concerns (WIPO, 1999).

As an institution, ICANN had notable success in its move to organize a rapidly expanding market around an epistemic community that managed to generate global norms in such a way that they became both willing to compromise on issues and follow the eventual outcome of decisions taken within that group. This also effectively geared the priorities of the Internet Governance regime towards technical aspects and the market itself, rather than focusing on State interests (DENARDIS and RAYMOND, 2013).

It is important to highlight that ICANN does not sell any particular item, but rather acts as the designer and manager of contracts that bind a long chain of intermediaries so that they remain aligned with the norms set by its multistakeholder community. The sale of domain names and related activities are handled mostly by ICANN-approved parties called registries and registrars, which operate independent from the institution but are legally bound to it (DATYSGELD, 2017).

To the United States, this must have been an interesting proposition. A body perceived as legitimate by a reasonable amount of players was established, being vested with the power to control core resources of the network in a shared manner, turning the governance of the Internet into a global endeavor. At the same time, it still allowed the US government to exert a superior amount of oversight by means of ICANN being contracted by the National Telecommunications and Information Administration (NTIA) to operate the IANA functions, instead of them being transferred over to ICANN.

This model thrived, growing steadily more active over time, as ICANN's position as the only legitimate DNS root of significance turned from an abstraction into reality,

and power structures consolidated around the institution. Christou and Simpson (2007) very aptly define the capacity derived from this arrangement as "international policy implementation through gate keeping", a concept that in our research has been condensed under the term Guardian Policy[2].

What we implicate by Guardian Policy is that the norms established within ICANN's community have a direct effect on the Internet as a whole by means of the DNS, in such a way that any actor that wishes to take part in the network is obliged to implicitly accept or at least actively engage with those norms. This is significantly different from what happens in most other international institutions, where in spite of diverse coercive measures, at the end of the day it is up to the actor to accept or deny a norm.

To us, this demonstrates a substantial *enforcement* capability by ICANN's part, one that, within the limited scope of its influence, is comparable to that of government-sponsored institutions. To better qualify the use of the term enforcement here, we base our argument on an understanding synthesized by Scott Anderson, that aims to differentiate the practice of enforcement from the more unassuming attitude of pressuring an actor. He writes:

> This earlier approach to coercion – which I will call the "enforcement" approach – regards coercion as a kind of activity by a powerful agent who creates and then utilizes a significant disparity in power over another in order to constrain or alter the latter's possibilities for action. This power differential may be used to put pressure on the coercee's will, but additionally it might work by simply interdicting or disabling agents, or disrupting various possibilities for action more systematically. Such systematic disruption can be achieved by incarceration or capital punishment, as well as via longstanding threats that alter broad patterns of activity, and not just specific actions *(ANDERSON, 2010)*.

While no capital punishments have been recommended by ICANN, the institution has found success in mediating disputes over contentious domain names, steering the focus of an entire industry, and convincing relevant actors from all sectors to participate in its regular processes. Not only that, but using the relatively modest toolkit of the IANA functions, this institution has been able to influence matters that transcend the technical and step into the political.

An often cited example of how ICANN can succeed in advancing contentious subjects is the ".xxx" suffix, tailored towards adult or pornographic content. This domain was implemented into the DNS root in spite of the sensibilities of some stakeholders, such as highly religious States, and what this amounted to was that a technical decision ended up validating the right to consume adult material on the Internet, leaving States

---

[2] "*Política do Guardião*" in the initial research published in Portuguese.

to censor such domains on a national level if they so desired (KURBALIJA, 2016). This brings us back to our previous point that governments are compelled to engage with ICANN's norms, even if it is to impede them from being used within the limits of their sovereignty.

Let us briefly recall that the multistakeholder model in often considered an enhancement over transnational processes of norm-setting, filling gaps left by ordinary politics and opening an avenue for consensus-based decisions that might not please all of those involved, but still partially satisfy everyone enough to turn the compromise into a manageable norm. This should, in theory, also be the outcome of multilateral processes, but most examples we have do not point towards that direction (DENARDIS and RAYMOND, 2013).

Other authors interpret multistakeholder arrangements as an artifice utilized to create a perception of coherence and homogeneity between diverse interest groups that exist inside of complex issue areas, in such a way that actors with the highest economic strength manage to push more of their interests into decisions than others, generating a system that is more favorable to them while keeping a façade of inclusion and dialogue (HOFMANN, 2016).

During our research we did find compelling evidence that Internet Governance differs from comparable multistakeholder arrangements in significant ways. Highlighting insights from our study of both the International Organization for Standardization (ISO) and the *Fédération Internationale de Football Association* (FIFA), it becomes clear that despite both of them seeing active transnational involvement of actors other than governments and possessing some form of enforcement capability within their competences, the State actor still remains the protagonist within them.

This happens due to the fact that filiation with ISO and FIFA depends on a person or company being part of closed national groups that are sanctioned by the governments of each participating country. This does not allow for a party that has relevant knowledge, information or interest to be able to intervene in the process out of their own volition, needing to first receive direct or indirect clearance from their government.

Using Brazil as an example, the Brazilian Association of Technical Standards (ABNT) represents the country in ISO, while the Brazilian Football Confederation (CBF) is the representative in FIFA. Both institutions are supervised by the government and therefore must remain generally aligned with its interests. Meanwhile, in ICANN, IETF, W3C and the IGF, any Brazilian citizen with an interest in ongoing debates may join almost every mailing list and attend nearly all sessions in face-to-face meetings, with the exception of a handful of closed ones.

During our field research, an opportunity was requested from ABNT to attend an ISO meeting that was to take place in the city of São Paulo. On March 2, 2017, we received the following answer, translated into English for the interest of this paper: "The international meeting ISO/TC 199 is totally technical in regards to the security of machines and equipment. To participate in the meeting, it is necessary that the interested party takes part in the meetings of the study commission (CE-004:026.001) and also be associated with ABNT (as an individual or business, and in the case of businesses, a representative must be appointed to take part in the meetings). As the São Paulo State University is not a member of the study commission that elaborates those technical norms, according to the ISO and ABNT procedures, your participation will unfortunately not be allowed".

Looking at another example, the Forest Stewardship Council (FSC) is considered one of the most relevant multistakeholder institutions in the world. Active since 1993, it sought to set standards on forest originated products, using a *tripartie* structure that balances the positions of industry, environmental NGOs, and social groups, in such a way that NGOs and social groups are always at a majority position. In spite of that, when it comes to the actual enforcement of norms, the industry often gets away with not acting in alignment with decisions, as there is no mechanism for those norms to be globally enforced, and watchdogs lack the resources necessary to thoroughly investigate potential violations (MOOG, SPICER and BÖHM, 2015).

To bring this information back into the context of Internet Governance, it is possible to observe two key areas in which it stands out: first is the degree of openness in participation, which allows for the inclusion of any actor that feels affected by an issue, regardless of any criteria that might block their participation. Second, and even more important, ICANN's Guardian Policy allows for it to centrally enforce norms, in such a way that evading them requires actors to go out of their way in very significant manners, and even so, at a global level what matters most is the DNS as provided by the root servers.

So, where do States fit within Internet Governance? Assuming that there is a dichotomy between top-down and bottom-up approaches to norm-setting, it follows that the first option is more widely associated with States, while the second can generally be observed within multistakeholder institutions such as ICANN. While States have traditionally been the leading actors in the generation of norms that have a transnational impact, the set of variables surrounding Internet Governance has made considerable dents in the norm-setting capacities of States within this arena.

It makes sense, then, that there would be friction between State actors and the remaining stakeholders that compose Internet Governance. While on one hand civil actors from around the globe — even gigantic corporations — are expected to follow norms set by the States in which they reside or operate, on the other hand the State

actors are generally not expected to voluntarily obey arbitrary norms set by civil actors, even more so if those norms are set by foreigners. The process of ratifying an international agreement carried out by a State's executive branch is a mere formality in other arenas, due to the further need of approval by their legislative bodies. Here, however, it carries real weight.

This setup led to a late reaction by governments which assembled under the United Nations umbrella, in what became known as the *World Summit on the Information Society* (WSIS), which was made up of two main meetings: 2003 in Geneva and 2005 in Tunis. It is notable by studying the tone of the discussions carried out that these meetings represent a reaction by other States to a perceived monopoly held by the United States together with ICANN[3] over matters of Internet Governance.

There are two main takeaways from this process: the recognition by States of the multistakeholder model for Internet policymaking and the creation of the Internet Governance Forum (IGF), intended to be a space for the debate of global public policymaking, more or less acting as a placeholder and seizing that niche before ICANN or high-ranking members of its community could take a stab at it, preempting a turn of events such as the one that transpired on the technical level. This is particularly evident when one evaluates the language being employed, proposing that there was a "vacuum" to be occupied for matters of public policy (WGIG, 2005).

It is interesting to note that the term Internet Governance was not even being used by governments in the preparatory assemblies for the WSIS. However, by the Geneva meeting, a mindset had been established that this was the ideal language to be used. Also, some of the States most actively participating in the discussion were Saudi Arabia, Iran, and Cuba, among other actors not particularly interested in the openness of the Internet, denoting that by then a feeling that this was becoming threat to the sovereignty of non-democratic governments had been established (DENARDIS and RAYMOND, 2013).

Reflecting the tendency of States to build mechanisms incapable of binding them, the IGF follows a structure of community Workshops that are meant to debate and coordinate matters of content and participation on the Internet, but it is not sought to form any manner of broader agreement or even achieve a set of deliverables. In this manner, a policy discussion space was occupied without really attempting to establish a global arena for Internet policymaking that transcends the technical, maintaining individual State oversight over what content is allowed under their sovereignty. That also partially mitigates ICANN's power by affirming that the corporation should not touch upon matters of content.

---

[3] It could be argued that within this thematic and during the timeframe being discussed, from the perspective of State actors, United States and ICANN were terms that could be used interchangeably.

2. Legitimacy, power, and the occupation of conceptual spaces

ICANN managed to exert enough influence within its names and numbers niche that it sidelined States into a position of being non-voting members of their Board of Directors. This is by no means an outcome that should be accepted casually, and in order to better understand how that took place, we have selected 3 key points to analyze. They are: A) examine the formation of the DNS per se and why it provides a measure of power to the actor that controls it; B) evaluate how legitimacy was established by the actors who took on leading positions within the Internet Governance regime; and C) understand how subsequently the dynamics between State and private actors in this multistakeholder environment were consolidated.

To accomplish this, we need to first look towards the origins of the Internet Governance regime, when Jon Postel received in 1977 the task of curating the root server that operated a primitive version of the DNS at the Stanford Research Institute, which at the time only allowed for non-commercial addresses that were added by hand to the root. At that time, a single table inside a file named "HOSTS.TXT" was responsible for the coordination of connections happening around the ARPANET, which might seem like an overly simple solution for establishing a root authority, but proved to be a key factor in allowing networks to leap from a model in which there was no universal taxonomy for domain names to one in which all could share addresses following a common structure, without the risk of name duplication (WU, 2008).

Initially, operators would download the root file to service their own networks on a nightly basis, but this became problematic due to the fact that many systems that were initially purpose-built and isolated began to connect and assemble under a single network, and this method was not scalable enough to account for the increasing demand. Difficulties were encountered particularly when it came to delivering e-mail messages with accuracy and speed, which made it observable that a new approach was necessary. A series of RFCs were drafted, culminating in 1983 when the concept of the DNS as we understand it today was designed and implemented with the potential for expansion in mind (MOCKAPETRIS, 1983).

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. At that point, a general understanding was also reached about how to carry out the expansion of the network on a physical dimension, with State actors fronting the costs associated with the common infrastructure that was necessary (LEINER, CERF, *et al.*, 2012). Seeing as NSFNET recognized the Stanford Research Institute as the root, this further consolidated the position of that actor under the role of legitimate provider of names on the Internet.

By this point, the root server had been elevated to what some would come to define as one of the "critical Internet resources"[4]. While nothing impedes the Internet from operating without a root server for domain names, at the same time there are many factors that favor its existence. As part of a globally shared resource, it is vital that there be no ambiguity in the address of websites and e-mail servers, in order to avoid misleading, dangerous, and technically inviable situations. On top of that, while underlying IP addresses[5] might change for varied reasons, a domain name should in general remain stable over time, enabling access by users independent of changes performed to servers.

In 1992, ISOC was founded in Switzerland, predominantly by players who had engineered some part of the global network during its formative years. This nonprofit institution had the objective of providing a governance structure for the Internet, being a nexus of discussions concerning its steering, as well as privately financing projects in a manner that was independent from governments. This position did not please the Clinton administration, which saw the United States as the financier and developer of the project, and thus considered that the US government was entitled to a central role in the governance of the network (MUELLER, 2004).

Partially in answer to the creation of ISOC, the United States government put control over the root servers up for auction, leading Network Solutions Inc. (NSI) to assume their curation in 1993, transferring stewardship over the network from academia to the private sector. Postel's legitimacy carried such weight at that point in time that he was maintained as policy coordinator, while NSI operated the practical aspects of the DNS. Following these changes, a resolve was eventually reached that allowed for the sale of domain names, carried out on a first-come-first-served basis and at a fixed cost starting from 1995. This was the catalyst to a process that would make it so that in a few years the domain names market would be worth around 200 million dollars, up from zero (WU, 2008).

Many events came together for that market boom to be made possible, of course. Starting from 1991, the wider adoption of the World Wide Web (WWW or Web) made it conceivable for people with less technical knowledge to engage with the Internet. Even if it was still quite focused on the academic community, there was already a nascent interest by businesses and civil society actors in making use of that technology. In Brazil, this was observed during the lead-up to the United Nations Conference on Environment and Development (better known as RIO-92), when part of Rio de Janeiro was networked with combined efforts between academia and civil society, to serve the

---

[4] A language that has been, for instance, adopted by the United Nations, as can be observed in the Main Session of the 6th IGF, entitled "Critical Internet Resources".

[5] Not only IP addresses, but any other numerical or reference value set at the machine level. Therefore, this would still apply even under a different protocol suite.

purpose of increasing awareness and providing higher quality real time coverage for the massive event (KNIGHT, 2014).

The year of 1995 is particularly relevant when we consider the commercialization of the Internet, seeing as Microsoft released Windows 95, which brought an exceptional combination of affordability and a low learning curve to the home user, with its entirely graphical interface and relative wealth of features. Later in the same year, a Service Pack was released with built-in support for TCP/IP and the second version of the Internet Explorer browser (MORRIS, 2015).

It is also important to highlight that, in the same year, the Netscape browser brought along several innovations to the Web, out of which the Secure Sockets Layer Protocol (SSL) stands out as the most relevant. It is interesting to note that this protocol was not developed by the already well-established IETF, but rather in-house by Netscape coders, and it still moved on to become a solid global standard anyway. SSL was a practical and safe solution that allow for monetary transactions to take place on the Internet, which motivated forerunner digital companies to invest in this suddenly viable business model (NAUGHTON, 2015).

The ".com" TLD, which had existed before as an identifier of the minimal space of business actors within the network, soon became the gateway for them to participate in the Web revolution. A previously barely feasible revenue stream turned into a potentially very relevant part of business strategies, and with this opportunity open, all manner of innovative ideas and services flourished, some more successful than others (LITMAN, 2000; TEETER and SANDBERG, 2017).

All of this did not go unnoticed, and securing control over the digital space became more important than ever, which takes us to the matter of the DNS Wars. While the DNS system remained within the jurisdiction and sovereignty of the United States government, ISOC maintained its claim to the responsibility for the governance of the Internet, and was directly questioned by said government about what vested them with the legitimacy to make such an assertion. The institution provided the measured answer that control over the Internet could not belong to a single State, and that they would like to inherit NSI's functions to better reflect a global arrangement (WU, 2008).

Between 1997 and 1998, ISOC expanded their efforts in order to bring together hundreds of supporters from different stakeholder groups that were sympathetic to the idea of having ISOC occupy a central role in Internet Governance, as well as receiving support from the United Nations and intellectual property organizations. In what was positioned as a form of "voluntary multilateralism", arrangements were made for the transfer of stewardship to take place as if it was a given (MUELLER, 2004).

The commercialization of the network was creating all manner of disputes at a practical and philosophical level, and with the favored position of the US in the

arrangement, it follows that the doctrine adopted to consider these matters would be very focused on the traditions of that State. One of the key objectives of the group led by ISOC was to move away the nexus of power from the United States to what was considered a more neutral ground in Geneva, so that processes relating to the network would "have an international orientation; not to be US-centric" (HEATH, 1997).

However, the fragility of the arrangement was exposed when the United States government simply did not give in to the pressure, refusing to transfer any function to ISOC, and as a result dismantling their initiative. Postel made a further attempt at challenging the government's legitimacy by staging a redirection of the DNS root to his own server, but the government forced its hand and he was compelled to undo the move (WU, 2008).

This attempt at legitimizing themselves at an international level in order to assert control over the DNS has a flavor that is distinctive of the 1990s, in a post-Cold War reality in which globalization was on the rise and boundaries seemed to lose their meaning for a fleeting moment, something that was in no short part helped by the Internet. Global Governance was on the rise, and ISOC's proposal rested on the backs of United Nations-centric initiatives such as the Commission on Global Governance and their "Our Global Neighborhood" document, fostering a sense of universal camaraderie and the betterment of society as a whole. If this sounds similar to what we proposed as one of the fundaments on which Internet Governance was built by its counterculture influenced leaders, it is no coincidence (DATYSGELD, 2017).

ISOC's proposal ended up not having the desired effect, and that particular initiative did not move forward, but this does not mean that a commotion hadn't been generated around the subject. The United States government proposed the formation of a new entity to control the DNS root, under the condition that it was housed within their territory and wasn't geared towards profit. Their proposition was that the process should be privatized and competition should be stimulated on the domain names market, while at the same time inclusivity towards the international community should be fostered in the norm-setting process (WU, 2008).

In 1998, ICANN was assembled, backed strongly by corporate players that wanted to achieve the growth of business on and around the Internet. It should come as no surprise that several actors involved in ISOC's proposal were carried over to this new arrangement, and Postel was to be brought back to the leadership of the new institution, something that never materialized due to his sudden death. The solution that was given to the DNS Wars was a manner of forced compromise in which the United States government asserted its position as a sovereign State and refused to be sideline by a coalition, only conceding to the demands presented by the community once its own needs were met (MUELLER, 2004). While this can be seen a win by the State actor, it is still impressive that the private sector managed to exert such influence.

The necessities of actors that were at the margin of that agreement were not directly addressed by either proposal, being touched upon in spirit under the umbrella of the "global community". The interests of States that did not belong to the Global North were an afterthought, and the arrangement was essentially one between different nexuses of power originating from the United States. The axis of tensions laid between North America and Western Europe, much like it had been in all previous disputes over global communications (HOFMANN, 2016; DENARDIS and RAYMOND, 2013).

When looking for a unifying thread that binds this sequence of events, we cannot help but stress that, over the years, Postel had been crowned the *de facto* authority over the root server and the broader "names and numbers" arrangement. For a long time, it was his task to add new legitimate addresses to the DNS by hand on demand. While nominally this was the responsibility of the university he worked for, it was more or less still a worldwide public service that had been entrusted to a single person.

While it is hard to assess something as intangible as influence, Postel seems to have channeled many of the ideals championed by the Internet pioneers that informed a structure that was so devoid of State actors. This, of course, could only be accomplished due to the fact that he was surrounded by likeminded people who shared a similar background. Had commercial or espionage interests become more prominent earlier, he would probably have been put aside by other powers.

ISOC hosts a list of 265 individual condolences given by people from the technology sector upon Postel's death in 1998, at the age of 55, from complications resulting from a heart surgery. Several of the entries in this list refer to him as the most important figure of the Internet at the time (ISOC, 1998). He had a decisive role in not only the establishment of IANA, DNS, and RFCs, but also in the creation of ISOC and ICANN. An article published on The Washington Post two days after his death echoes this sentiment:

> Postel's death comes at a critical juncture for the Internet, with the federal government in the midst of largely turning over management of the worldwide network to a nonprofit group that Postel helped organize. Although Postel was hardly known outside high-tech circles, his role as director of the Internet Assigned Numbers Authority allowed the Internet to match unique numerical addresses for computers on the global network with its millions of Web addresses. The British magazine The Economist once dubbed Postel "god" of the Internet *(THE WASHINGTON POST, 1998)*.

These are important considerations to have in mind as we move on into analyzing how control over the virtual space was obtained. This subject has been explored in the past by other commenters, so the effort of this paper in this regard is to bring the question into the light of Weber's "Three Types of Legitimate Rule", comprised of Legal

authority, Traditional authority, and Charismatic authority (WEBER, 2004). We feel that this is an interesting methodology to approach the problem, one that adapts with particular ease to a context where the political interests of different actors intersected in the space of ideas, and in which legitimate ownership was the main issue to be tackled.

We propose that ISOC, along with its partner associations such as the IETF and the multitude of academic interests behind them, sought legitimacy by means of traditional authority. Their claim to the DNS root was based on their technical capabilities and historical involvement in the subject, something that governments could not directly claim for themselves, at least not on the same scale. Those were the architects of the project that had controlled it for as long as it had existed, and in large part had steered the decisions that pertained to it. Their claim was, then, that the Internet had traditionally been their domain, and should continue to be for the foreseeable future.

However, this group sorely lacked legal authority. They never had any formal guarantee of their permanence in this position. The United States government always made sure to intermediate the development of the Internet through its government agencies and universities pursuant to contracts with the State. While it had indeed distributed the power of the Internet structure, it never really ceased to exert ownership over it, even as other countries' networking efforts became big enough to connect with *their* network. From a legalistic perspective, the United States was the financier, and for all purposes, the developer of the Internet, who had employed contractors to perform the job. This is why ISOC sought to align itself with State-sponsored ITU, who could grant them an added layer of legal authority.

When ICANN was forming, it could still rely on its traditional authority claim due to Postel's protagonism in this niche, but with his passing, it suddenly became more complicated to count on that. This prompted a heavier lean on charismatic authority, with figures that blended technical capacity with approachability — and here we need to point at Vint Cerf as a prime example — to strengthen its legitimacy. It became more important for the charismatic layer to be made present, which we assume had a direct impact on how ICANN's community was shaped. When the institution managed to combine the three types of rule under it, with the backing of the United States government, it became possible for ICANN to be born as a manager of the DNS root, while still being attached in more ways than one to its home government.

Incorporated in California, ICANN has established a narrative supported on it being a "global" — rather than international or transnational — institution, with the aim of serving the "public good". This greatly informs its position, showing an attempt to reduce ties with States and place its industry-led philosophy on top of the sovereign interests that occupy norm-setting processes such as those of the United Nations. This

can be observed in a brochure named "Who Run the Internet?", in which the institution defines itself in the following manner:

> The Internet itself is a globally distributed computer network comprised of many voluntarily interconnected autonomous networks. Similarly, its governance is conducted by a decentralized and international multistakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities, and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good *(ICANN, 2013)*.

Some successes achieved by ICANN operating under this arrangement are notable. It decentralized the domain names market, generating competition and a decrease in the cost of domains for the end user. It also established a fairly reliable mechanism for dispute resolution within the DNS. More than that, it allowed for the establishment of a scalable and stable system that is credible and not likely to collapse, as the dependability of the structure has been proven time and again (WU, 2008). More than one group within ICANN and the IETF is dedicated to the endurance of this stability, with constant tweaks being made to ensure the resiliency of the DNS.

Then again, the Guardian Policy can be carried out exactly for that reason. ICANN became the only actor capable of allowing something to be represented on the Internet with consistency and global reach, be it an individual, corporation, nation, or even an idea (CHRISTOU and SIMPSON, 2007). In other words, if it is decided within the institution that something does not agree with established norms, the multiple contracts that bind registries, registrars and those who contract their services to the United States and California come into action and allow ICANN to enforce whatever action has been deemed suitable by its community.

It is important to consider the dependency that ICANN had for most of its existence towards the Department of Commerce of the United States, which had the unique power of being able to veto a decision made by the ICANN community as a last ditch resort — and let us be clear here that as far as we known, this was never carried out, at least publically (TELEANU, 2016). It was not, however, such a clear cut matter that the IANA functions couldn't be taken away from them, and it took much effort and money from the institution and its community to move away from that situation in 2016's transition, in which it formally severed its ties to the Department of Commerce.

We know from veto player theory that departing from the *status quo* depends on achieving a suitable "winset", and that the existence of a single player that can veto all others has a very substantial impact on the process itself. In this way, the mere presence of the actor in itself limits departure from the *status quo* (TSEBELIS, 2001). In other words, while ICANN may not have been directly vetoed by the United States

government in regards to any particular policy, the very existence of the possibility of a veto has a chilling effect on attempting a departure from the expectations of the veto holder.

These are not the only structural concerns that should be raised. According to ICANN'S financial plan for 2017[6], the institution employs less than 400 people, out of which the majority exerts social, financial or maintenance functions. The deliberations that inform the norm-setting process are carried out by an open and global multistakeholder voluntary community that reunites both face-to-face and virtually to discuss their positions regarding issues that involve ICANN'S competences. The physical meetings take place three times a year, in a location rotation system that seeks to diversify regional participation, although the rotation is not quite predictable, and regions will repeat before another has the chance to be the host, for instance.

This "global multistakeholder voluntary community" is a double-edged knife. If on the one hand they add variety to the pool of opinions available for policymaking and are able to bring to light matters that initially may not seem relevant to other actors, on the other hand one must allow the fanfare to die down and have an honest look at who is really taking part in discussions. We raise this question for several reasons. First, the physical meetings are a core part of the norm-setting process, in which discussions carried out over mailing lists often take a different shape or reach conclusions. While nearly universal remote participation exists, it is quite different to engage in the discussion from the outside, even more so because many negotiations happen face-to-face, on the hallways in-between sessions, or during networking events. This creates a clear disadvantage to stakeholders participating remotely (DATYSGELD, 2017).

While there are scholarships and funding opportunities available, one has to ponder the difference between an actor with fixed funding whose sole function is participating in multistakeholder forums — as is the case with representatives from quite a few governments, businesses and NGOs — and an actor whose participation is sporadic and dependent on having funding requests approved or the use of their own resources. This also applies to the time factor, as online discussions that may take upwards of hundreds of hours in some cases will, by simple logic, see more action from actors who hold these tasks as primary or nearly primary functions. This, it seems fair to say, amounts to the existence of many "hired volunteers".

The tendency of actors that manage to find a structure to support them within Internet Governance is to remain where they are. A significant number of people who saw the birth of Internet Governance and ICANN have assumed long-standing roles and

---

[6] Available at <https://www.icann.org/en/system/files/files/proposed-opplan-budget-fy17-05mar16-en.pdf>

taken control of eminent spaces within that broad community, or continue to exert influence indirectly by affiliation with government or industry.

There is nothing specifically wrong with that. It is inherent to the multistakeholder model that each group of actors will have their own characteristics and capabilities, and maybe increased access to social media by civil society players can offset to some degree matters of participation, to give a hypothetic example. However, the crux of the matter is how this model is sold as an open and egalitarian arena, when in reality there is much more to be considered when we discuss legitimacy and participation. Cerf (2013) affirms that "stakeholders must realize that Internet Governance is not free", when discussing the IGF, but this might as well be a credo to be observed whenever evaluating any multistakeholder arrangement.

The complexity of the system is also not something to be ignored. The division of the community based on sectors — the Support Organizations and Advisory Committees, as well as the smaller Constituencies — generates a need for policies to be at a first moment discussed between peers, then taken to the broader community, and finally shaped to be recommended to the ICANN Board, whose members are really the ones who decide if a norm will be implemented or not. To exemplify this convolution, the Generic Names Supporting Organization (GNSO) has 15 distinct steps that need to be followed for the formation of a recommendation to the Board (HOFMANN, 2016). It is debatable whether Internet Governance was meant to be scalable up to the point it has reached in the late 2010s.

We see then that the Board is the final link in the chain that generates the institution's output, seeing as any set of decisions that ends up being sanctioned and turned into norm has to be approved by its members, who are by and large elected from the community. The most relevant fact to be noted is that the Board reserves the right to deny any suggestion made to it. While this certainly carries a political cost, at the same time there is no particular consequence to doing so as there is not an official higher instance for them to answer to (MUELLER, 2004).

The Board does not run on a voluntary basis, but rather employs 15 people that may be remunerated for their work[7], and together with the CEO they represent the interests of the ICANN community to the broader Internet ecosystem. The first Board was appointed by industry insiders, and after a few attempts at democratic election, the process that was decided upon involves selection by the Nominating Committee (NomCom), a specialized organ made up of a rotation of individuals that are considered trustworthy by the community (KWALWASSER, 2009).

A candidate cannot put himself up for the position of Board member, and is dependent on being nominated by somebody else. This is also the case in quite a few

---

[7] Each member has a choice to receive the salary or abdicate from receiving it.

other leadership positions within the community, but in the case of the Board, the process is much more rigorous and therefore support needs to be stronger. From our interview with a former NomCom member, we gathered that the procedure is as follows: after the candidature is sent together with three expressive references, the candidates are anonymized, so that they can go through a blind examination; this is done to preserve the privacy of those who are not selected. After diversity criteria have been applied, the candidates move into a phase in which they need to prove to prove themselves to the committee, both in virtual meetings and during ICANN meetings. In parallel, the NomCom does a deep dive in the candidate's public life, looking towards establishing their motivations and expressive contributions they made (DATYSGELD, 2017).

Members go in and out in an asynchronous manner, serving terms of three years that can be renewed or cut short if the need arises. Backup candidates are chosen by the NomCom in a secret manner, in case there is desistance or an unforeseen event; these candidates are not revealed to the community. Among qualified candidates, the decision of whether somebody becomes a Board member or is put on reserve is most of the time related with diversity criteria (DATYSGELD, 2017).

While flaws with this model could be pointed out, it does seem efficient enough in creating incentives for candidates to distance themselves somewhat from their constituencies and perform work that is meaningful for ICANN as a whole. Nothing stops them from serving an agenda after overcoming the selection process, but it can be affirmed that measures to mitigate conflicts of interest are in place and that there is an underlying intention to be transparent in the process.

It is our belief that what has been exposed so far is enough to at least rapidly cover the elements that constitute legitimacy within Internet Governance, and that the role of some relevant actors has been adequately contextualized. Therefore, looking back at our established goals, we had proposed to look at: A) why the DNS provides power; B) how legitimacy was established; and C) the dynamics between State and private actors.

As far as the first point is concerned, the power that is contained in the DNS originates from it being by far the most accepted point of reference for indexing addresses online. This status was not consolidated overnight, but rather had the confidence in it built over the course of decades, as a result of the efforts of many actors who developed the DNS both in terms of code and politics.

To the second point, the actors that assumed initial leading roles in this agenda came from the academic and government sectors, and were almost exclusively from the Global North. Within this limited community, they set more collectivistic governance standards that remained more or less stable until the commercialization of the Internet,

when an influx of private actors and global stakeholders became interested in it. This triggered a power struggle, which led the US government to opt for a middle ground in which it relayed control over the DNS to a global community while still maintaining oversight. Protagonists have remained largely the same ever since then.

The final element of this analysis, that of the dynamics between State and private actors, will be studied in the next section. We will attempt to understand both where States are expected to fit and where they wish to be positioned, along the way analyzing both their participation in ICANN and the creation of the UN-mandated Internet Governance Forum.

3. The participation of States in the Internet Governance regime

From the start, governments were not sympathetic towards the multistakeholder Internet Governance model, which presented itself as something distant from the set of procedures that they were used to follow. As far as the other actors of the regime are concerned, though, this model is the golden standard for the discussion of global Internet issues, and there are already too many economic, social and political interests involved for it to be put aside (KIGGINS, 2015).

As we discussed previously, the most prominent State actor throughout the Internet's formative decades was the United States government, with the governments of a few other European countries also playing significant roles that at the end of the day dwarfed in comparison to the privileged position that the US ended up having in the maintenance of the network of networks, serving not only as a political nexus, but also as the territory in which many relevant servers that operate popular services were located, a reality that still holds true today.

With the commercialization of the Internet and its subsequent rapid expansion, other government actors made a late arrival to the regime, causing mistrust in those who had already been part of the Internet Governance community. An anxiety arose from the idea that what State actors sought was to limit, censor, or eventually co-opt institutions such as ICANN (KIGGINS, 2015). This impression was not eased by the relative pomp and circumstance demanded by them upon their arrival, as we will see below.

The participation of government actors in ICANN takes place mostly by means of the Government Advisory Committee (GAC), whose stated purpose is that of giving advice relative to matters where public and private policies intersect in relation to the DNS. Its members "shall be national governments, multinational governmental organizations and treaty organizations, and public authorities, each of which may appoint one representative and one alternate representative to the GAC", with it being that "membership is open to all national governments. Membership is also open to distinct economies as recognized in international fora" (GAC, 2017).

A large part of the delegates that regularly attend ICANN meetings are in some way connected to the governmental structure of their home country, though that is not always the case. Some delegates are third parties acting under contract with the executive branch of a nation, and may not regularly exert any diplomatic function, but rather be specialized in technology in a way that is relevant to the debate that goes on within the GAC (DATYSGELD, 2017).

The dynamics of this group are distinct, as GAC meetings adopt a manner of assembly that is closer to what one would find at a United Nations gathering. Instead of the round table structure employed by groups within the GNSO, the GAC has a main

table where the chair and the vice-chairs seat, overlooking the other national representatives. They adhere to a stricter agenda and have as an aim at the end of their physical meetings to draft a *communiqué*, an open letter in which the intentions of the group are affirmed to the Board.

Established in 1999, this body occupies the Advisory Committee category, denoting that the collective of actors involved in it may recommend actions directly to ICANN's Board once consensus is reached by governments. In this sense, the varied Support Organizations – made up of civilians that represent the interest of commercial and non-commercial users and compose the bulk of ICANN – have mostly the same degree of privilege as State actors, so it can be said that stakeholder balance is achieved in structural terms.

On the other hand, looking at the Board of Directors gives us a different picture. Out of its 19 members, 15 fall within the category of Voting Directors, while 4 are Liaisons. Voting seats are mostly occupied by members of SOs, together with the ICANN CEO and a handful of seats reserved for ACs. The GAC, however, occupies one of the non-voting Liaison chairs, and therefore does not exercise a direct influence on the definition of norms once deliberation has been done by the community. They can strongly voice agreement or disagreement, but that still does not change outcomes.

The number of GAC members was quite small at the beginning of ICANN, partially reflecting the fact that most governments did not really grasp the relevance of the Internet at that early stage and partially because it was assumed that the issues being discussed there were better left to the technical community, as they would not really escalate to a level of relevance that would upset States. In due time, that changed (HYPPONEN, 2013).

Initially, the GAC acted separately from the rest of the community, both intellectually and physically, keeping a distance in their affairs and considering their position as distinct from that which other constituents enjoyed. Their meetings were closed and did not have the same level of transparency that other stakeholders are held against, without recordings or transcripts being made of their sessions, for example (NOSS and GOMES, 2017).

In time, more State actors joined the GAC, and institutionally it underwent many changes. Parts of their meetings became open, accompanied by transcripts and audio recordings. Their methodology became more and more aligned with the remainder of the community over the years, which leads us to believe that States initially didn't really have a clear understanding of how to participate in a multistakeholder institution of ICANN's size, and expected that their role would be different from that of others. The process of the opening themselves to the community reached a high point in 2016, at the Marrakesh meeting, when the GAC held its first fully open meeting, all the way to

the communiqué drafting session which had been kept away from prying eyes for the previous decades (DATYSGELD, 2017).

A subtler face of States within ICANN are the Country Code Top-Level Domains (ccTLDs), which are made up of optional national suffixes such as for example ".fi" and ".mx", for Finland and Mexico respectively[8]. This group of actors has a heterogeneous history that is complicated to trace, seeing as initially Postel assigned the management of these suffixes on a personal basis to people that he considered to be "responsible". In this manner, control over them was usually delegated to science and education institutions rather than to governments themselves (MUELLER, 2004). Here we stumble once more into how Postel and his claim to legitimacy ended up shaping long term discussions that unfold to this day.

When ICANN established itself and began tying together all pieces of the DNS under a single management, they requested that ccTLD operators engage them in contract like all other actors did, but in this case, the operators refused. With Postel dead, the institution found itself short on legitimacy to exert enough pressure to make the holders of the ccTLDs relinquish their control, and as such, they became the most prominent actors to be a part of the DNS while keeping a rather light-touch relationship with ICANN. As Yu puts it:

> While ICANN expected ccTLD managers to enter into contracts in which the managers would acknowledge ICANN's authority and would agree to contribute fees to the organization, the managers refused. In response, the managers questioned ICANN's authority and criticized the organization for its lack of openness, accountability, and representation *(YU, 2003)*.

At first, the ccTLD operators were reluctant to come to ICANN meetings in the beginning, and felt they did not have an obligation to do so, something that changed significantly over the next decade. Some of the first conflicts that arose within their mandate were exactly related to some governments claiming legitimacy in ICANN over the operators to whom the suffixes had been entrusted (NOSS and GOMES, 2017). In time, tougher criteria for ownership was established, and a multitude of agreements were reached with varied outcomes, but in general the ccTLDs are still operated by institutions that are not organs of governments, but maintain formal relationships with them.

The relative freedom that ccTLD operators enjoy has led to a series of non-standard uses of the suffixes owned by different countries, which drove a lot of the innovation in the DNS sector before the introduction of New GTLDs (such as ".bar") in the 2010s. Perhaps the most notable out of them are Tuvalu, gifted with the coveted ".tv" suffix, Montenegro with the ".me" suffix, and Tonga with the ".to" suffix. A

---

[8] In order to define what a country is, Postel opted to use the ISO 3166-1 country codes list as the reference, so that political discussions on that matter would not become inherent to the DNS.

particularly notable use of a ccTLD outside of that list is how Google adopted Belgium's ".be" for the shortening of its video URLs under the form of "youtu.be".

Tuvalu sold the rights over its ccTLD to an US company that is responsible for selling domains with that suffix, and the nation has enjoyed yearly revenue in the millions ever since. As early as 1994 there had been interest in the use of ".tv" names by broadcasters, and the decision on how to capitalize on that was reached by the government after seeking advice from the ITU (rather than ICANN or other fellow operators) and was counseled to start a bidding process to license the use of the domain name for a finite amount of time, so as to hold on to their sovereignty in the long run. The deal ended up favoring Idealab, which in turn sold it to VeriSign. The upfront payment of that deal alone was valued at 10 million dollars for Tuvalu (BALDACCHINO and MELLOR, 2015).

It is important to mention that out of the Sponsored Top-Level Domains (sTLDs) round that took place in the late 2000s, a domain suffix that is neither a ccTLD nor a New TLD stands out, namely ".asia". In 2008, this domain pioneered what are now called geoTLDs, with an interest in promoting the image of the continent as a whole, not focusing on a specific State. To purchase a domain name with this suffix it is necessary to prove that it will be used for the benefit of Asians, and it has been adopted in particular by the ASEAN countries, and used for continental-scale marketing campaigns, events and businesses, and to denote intergovernmental or multilateral bodies in the region (DATYSGELD, 2017). Following ".asia", interest in geoTLDs picked up, as we will see further ahead.

While these are two important fronts in which State actors fight battles, it is clear that the GAC and ccTLDs are not the only avenues governments have available in order to influence policymaking, as they also sponsor experts to take part in the activities of other stakeholder groups in order to shape the input offered by them in a way that is more aligned with State interests. In Kwalwasser's opinion:

> Given this context, power—defined as the capacity to influence a particular decision or result—is difficult to quantify. For nations other than the United States, governments' power is constrained. Governments have no vote on ICANN's decisions. Their influence through the GAC has been weak. They may try to invigorate it, but that possibility remains an open question. Alternatively, they may be able to increase their influence by spending more time and effort participating in board committees or supporting organizations, although they would have no greater status than nongovernmental members. Whichever route they choose, their influence will have to come from the level of expertise and effort they put forward *(KWALWASSER, 2009)*.

In terms of concrete policies formulated by governments within ICANN, the matter that seems the most relevant is their contribution to the "Protection of IGO and INGO Identifiers in All gTLDs Policy". This set of norms limits the uses in the DNS of

names associated with the Red Cross, the International Olympic Committee, International Governmental Organizations (IGOs), and International Non-Governmental Organizations (INGOs), accounting for their names in several languages and scripts (ICANN, 2018). This is an interesting policy because it limits the ability of scammers to create websites that, for example, impersonate the Red Cross following natural disasters, in order to con people out of donation money.

Another question that the GAC involved itself deeply in is the emerging question of geoTLDs, with three cases standing out in particular: ".africa", ".patagonia" and ".amazon". For ".africa", after almost 10 years of debates and deliberations about who had the legitimacy to operate it, the domain name was authorized to be sold, but the momentum never quite picked up, and registration numbers are low. In the case of ".patagonia", the sports brand wanted to register the name, but after a strong negative response from the GAC led by Argentina, the application was dropped. The story of ".amazon" is similar, as it involves a brand in dispute with governments, but it is proving to be a longstanding dispute, with no defined end in sight.

A globally relevant matter that was eventually driven forward by governments is that of Internationalized Domain Names (IDNs) at the top-level, which allows for addresses to be presented fully in non-Latin (or non-ASCII) languages and scripts, such as Arabic, Chinese and Cyrillic. This enables greater ease of use for people interacting with the Internet outside of its Latin-using portion, seeing as this stops demanding that they switch input methods in order to be able to navigate to a desired URL, as long as the domain incorporates an IDN of course.

During the decade of 2000, IDNs at the second-level started to become a part of the DNS[9], meaning that the portion of the address which contains the website's name could already incorporate that feature under certain circumstances. However, the top-level part of the domain, including ccTLDs, was an entirely different matter, and took longer to get approved by ICANN. On top of that, "IDNs were poorly supported by Internet browsers and IDN email did not work at all" (TAYLOR, 2011).

There are complex technical matters behind why it is so hard to operate the Internet in this manner, but two of the main concerns are interoperability and security. The interoperability part is simple to understand, as systems which were not made to support those characters would outright fail to process them, risking the fragmentation of the DNS. The security part is perhaps even more relevant, though, because characters in certain scripts are very similar to an equivalent character in another, such as is the case of the Latin letter "i", which has an equivalent Cyrillic character. Functionally, a fake

---

[9] Under the Internationalized Domain Names in Applications (IDNA) protocol, developed under the auspices of the IETF.

domain could be created using the Cyrillic character to emulate another domain and potentially harm misguided users (DATYSGELD, 2018).

During ICANN's 27th meeting in 2006, the GAC and ccNSO were asked generate a report that would enable the advancement of IDNs at the top-level, and they proceeded to work under a joint umbrella named IDNC WG. After receiving input from the remainder of the ICANN community and going through the institution's norm-setting process, this resulted in the Board approving the launch of the "IDN ccTLD Fast Track" process in 2009 at its 36th meeting, taking place in South Korea (ICANN, 2009).

This was a very necessary move, one that arrived late if analyzed under proper context. This is due to the fact that informal solutions such as plug-ins to browsers that enabled the conversion of Chinese characters had already long been in use in China, but in 2006 the State began to move aggressively towards outright circumventing ICANN and deploying domains with full Chinese scripts under their authority, something that would violate the principle of maintaining a single and reliable root for the DNS (BRAY, 2006).

ICANN's process lagged behind the impressive demand for these domain names, something which can be proven by observing the Cyrillic version of the suffix for "Russian Federation" released in 2010, which saw over half a million registrations in a few days (ICANN, 2010). How many of those were speculators or actual interested parties – likely a combination of both – this still demonstrates very strong confidence in the demand for IDN domains.

As all of the processes mentioned in this section were unfolding within ICANN, governments felt pressure building up around other Internet matters, and decided to take matters into their hands before other actors attempted to. The Internet Governance Forum (IGF) was established in 2005 by the executive branches of a number of countries, as a result of questions raised within the United Nations regarding the US role in Internet Governance, which was perceived as being too prominent in the coordination of administrative functions of the network (DENARDIS and RAYMOND, 2013).

The IGF maintains the multistakeholder nature of the other Internet Governance institutions, but heads in a very different direction in terms of norm-setting. As in, it does not engage in norm-setting. The forum was conceived as a space for dialogue, and the negotiation of firm standards is not presumed. There is potentiality in this arrangement for benchmarks to be set, but in practice, the IGF has little influence on global policymaking processes and has limited reach. Hoffman (2016) is not an admirer of the multistakeholder model, but when comparing ICANN to the IGF, she is quite clear: "Unlike the IGF, ICANN is an example of a multi-stakeholder process that produces concrete outcomes".

Since its inauguration, the forum has caused controversy among non-governmental actors involved in the agenda for a number of reasons. Closed-door meetings were held in which key IGF organization matters were decided, which did not allow an assessment of how much the contributions made by the community impacted the decision-making process, putting in check its commitment to the multistakeholder process. A series of working groups devoted to the subject have managed to achieve significant advances in the inclusiveness of the community, but it remains open to interpretation how much of this can be translated into results (HOFMANN, 2016).

While a significant portion of the non-logistical steering of the forum has been moved into the hands of a group composed of Internet community members called the Multistakeholder Advisory Group (MAG), government participation itself has seen a decrease, and members of civil society made up 45% of the attendance of the 2017 edition (IGF, 2017). This is a consequence of State actors starting to look for ways to discuss these matters outside of multistakeholder approaches, finding ways to collaborate between themselves.

It can be said that even more broadly governments have been a seeking a way out, something that is best symbolized by Russian president Vladimir Putin's attempt at making viable a DNS for the BRICS bloc. While not aimed at replacing ICANN's system, it is intended as a sort of backup, which would carry on working in case of any attempts made to damage or meddle with the normal Internet operation of the BRICS countries coming from the United States side of the equation (MOODY, 2017).

If implemented, this would open a precedent for many other similar solutions that might make sense, such as a European Union DNS that operates perfectly in harmony with the tight constraints of their laws, or an African DNS that better accommodates the shut downs that many governments of the continent have carried out with increasing intensity, particularly around elections time. This would fundamentally change the dynamics of Internet Governance as we understand it.

Final considerations

When in 2013 the security expert and contractor to the army Edward Snowden revealed to the international community that the US government was practicing mass espionage of global communications systems, leaders of all major Internet Governance institutions[10] organized themselves to publish the "Montevideo Statement on the Future of Internet Cooperation", in which they denounced actions that would undermine confidence in the global computer network, and explicitly demanded the definitive transition of the IANA Functions to ICANN, continuing the process of detachment from the US government in favor of an accountable international institution (W3C, 2013).

The aftermath of the Snowden revelations triggered innumerable consequences within ICANN, with the end goal of reaching a definitive agreement about ICANN's relationship with governments. One case of note happened when the Cross-Constituency Working Group on Accountability that performed a series of analyses on the operation of ICANN in order to accommodate the IANA transition made a recommendation based on the results of the assessment named "Stress Test 18" that ICANN's Board was to take GAC advice only when it was achieved under majority consensus within that committee, so that ICANN would not act as an arbiter of government disputes. This was met with mixed results by governments, as it would mean the necessity of straining relations in order to achieve the required standard, but would also add more weight to eventual decisions. Ultimately, the advice was rejected by the GAC (ERMERT, 2015).

The transition finally took place in 2016, when the US Ministry of Commerce considered sufficient the guarantees given by the ICANN community on the matters of transparency and accountability. The process happened amid a very contentious presidential election in the US, and Republican party politicians led by Senator Ted Cruz argued that the Obama administration was handing over control of important Internet functions to states it considered authoritarian such as China and Russia (WHEELWRIGHT, 2016). This line of argument continues to emerge in other contexts, and will likely remain a source of leverage to be wielded against ICANN for the foreseeable future.

With the transition in place, ICANN finally became the supranational actor with control over the DNS that it wanted to be for the longest time, but if the community thought that it was in for a smoother ride, it was quite wrong. With the enforceable period of the European Union's General Data Protection Regulation (GDPR) fast approaching in 2018, ICANN still had not readied appropriate measures to accommodate the much tougher data privacy requirements set by the GDPR, particularly in relation to the WHOIS database, which stores personal data from every

---

[10] ICANN, ISOC, IETF, the Internet Architecture Board (IAB), the World Wide Web Consortium (W3C), and the five regional Internet address registries.

person or entity that ever registered a domain name, and all of that data was open for public consultation without any requirements (VAUGHAN-NICHOLS, 2018).

Over a decade of fruitless discussion carried out by the ICANN community over what to do with WHOIS, a consensus never manifested itself. On the trails of the IANA transition and still resolving issues from the first round of New GTLDs that had taken place years before, the needle never quite moved towards prioritizing GDPR, until it was too late, and without community consensus, the Board had to implement a temporary set of rules that basically forced the anonymization of WHOIS from the top-down. This was done in order to avoid a potentially ruining lawsuit from the European Union.

Taking the information outlined above into consideration, we see conflicting realities. On one hand, Internet Governance has made itself more independent from governments, while on the other hand it was forced by a set of States to ignore the due process that binds its community together. Gains and losses seem to outline ever-changing prospects, and questions about the scalability of multistakeholder arrangements still loom in the horizon, with ICANN being the best candidate to test just how the pieces of that puzzle are supposed to fit.

Looking at the IGF's limited role in norm-setting, we can conclude that the Internet Governance regime as currently established does not cover most issues related to the Internet. On the contrary, the space that has effectively been dominated by the private sector consists of a small part of an enormous network, but since ICANN is virtually the only source of norms with real transnational qualities that are not of a purely technical nature, the institution concentrates an amount of political power that is disproportionate with the scope of the issues that it proposes to deal with.

It remains to be seen whether it will manage to continue wielding this power advantage, as governments clearly move towards establishing stronger positions of legitimacy and sovereignty in all dimensions of the digital space. Transitions are happening in the institution as the founders of the regime start to retire, such as the significant leaving of RFC creator Stephen Crocker from the position of chair of ICANN's Board. Strong leadership and a stronger community will be necessary for the institution to hold on to its power. As it stands in 2018, the situation can be considered stabilized, but as proven by the GDPR, the situation can change swiftly, and continuous study of Internet Governance is necessary to better understand what this complex and fascinating regime is leading towards.

Bibliography

ANDERSON, S. The Enforcement Approach to Coercion. **Journal of Ethics & Social Philosophy**, Los Angeles, v. 5, n. 1, p. 31, out. 2010.

BALDACCHINO, G.; MELLOR, C. Tuvalu: Entrepreneurship and the Dot TV Phenomenon. In: BALDACCHINO, G. **Entrepreneurship in Small Island States and Territories**. Abingdon: Routledge, 2015. Cap. 16.

BRAY, H. China sets up system for Internet domains. **The New York Times**, 2006. Disponivel em: <https://www.nytimes.com/2006/03/01/technology/china-sets-up-system-for-internet-domains.html>. Acesso em: 2018.

CHRISTOU, G.; SIMPSON, S. **The New Electronic Marketplace:** European Governance Strategies in a Globalising Economy. Cheltenham: Edward Elgar Pub, 2007. 75-87 p.

DATYSGELD, M. W. O papel da Governança da Internet dentro da Governança Global: Um estudo de caso da ICANN. **Repositório Institucional UNESP**, 2017. Disponivel em: <https://repositorio.unesp.br/bitstream/handle/11449/151066/datysgeld_mw_me_mar.pdf>. Acesso em: nov. 2017.

DATYSGELD, M. W. Ameaças a nomes de domínio: typosquatting, doppelganger domains e IDN phishing. **MarkWD.website**, 2018. Disponivel em: <https://markwd.website/articles/s010pt-ameacas-a-nomes-de-dominio-typosquatting-doppelganger-domains-e-idn-phishing.html>. Acesso em: 2018.

DENARDIS, L.; RAYMOND, M. **Thinking Clearly about Multistakeholder Internet Governance**. Eighth Annual GigaNet Symposium. Bali, p. 18. 2013.

ERMERT, M. Governments' Role In Management Of Internet In Question At ICANN Meeting. **Intellectual Property Watch**, 2015. Disponivel em: <http://www.ip-watch.org/2015/10/19/governments-role-in-management-of-internet-in-question-at-icann-meeting/>. Acesso em: 2018.

GAC. GAC Operating Principles. **ICANN GAC**, 2017. Disponivel em: <https://gacweb.icann.org/display/gacweb/GAC+Operating+Principles>. Acesso em: nov. 2017.

HAFNER, K.; LYON, M. **Where Wizards Stay Up Late:** The Origins of the Internet. New York City: Simon & Schuster, 1998.

HEATH, D. Beginnings: internet self-governance: a requirement to fulfill the promise. **ITU**, 1997. Disponivel em: <http://www.itu.int/newsarchive/projects/dns-meet/HeathAddress.html>. Acesso em: 2018.

HOFMANN, J. Multi-stakeholderism in Internet governance: putting a fiction into practice. **Journal of Cyber Policy**, Milton Park, v. 1, n. 1, p. 29-49, 2016.

HYPPONEN, M. Cyber Attacks. In: BBVA **Change:** 19 Key Essays on How the Internet Is Changing Our Lives. Palermo: BBVA, 2013. Cap. 4, p. 108-122.

ICANN. Adopted Board Resolutions: Seoul. **ICANN**, 2009. Disponivel em: <https://www.icann.org/resources/board-material/resolutions-2009-10-30-en>. Acesso em: 2018.

ICANN. Russian IDN ccTLD.po Opens for Registrations, Makes History. **ICANN**, 2010. Disponivel em: <https://www.icann.org/news/blog/russian-idn-cctld-opens-for-registrations-makes-history>. Acesso em: 2018.

ICANN. Who Runs the Internet? **ICANN**, 2013. Disponivel em: <https://www.icann.org/news/multimedia/78>. Acesso em: mar. 2017.

ICANN. Protection of IGO and INGO Identifiers in All gTLDs Policy. **ICANN**, 2018. Disponivel em: <https://www.icann.org/resources/pages/igo-ingo-protection-policy-2018-01-16-en>. Acesso em: 2018.

IGF. IGF 2017 Attendance & Programme Statistics. **IGF**, 2017. Disponivel em: <https://www.intgovforum.org/multilingual/content/igf-2017-attendance-programme-statistics>. Acesso em: 2018.

ISOC. Condolences and Remembrances. **ISOC**, 1998. Disponivel em: <http://www.isoc.org/postel/condolences.shtml>. Acesso em: nov. 2017.

KIGGINS, R. Open for Expansion: US Policy and the Purpose for the Internet in the Post–Cold War Era. **International Studies Perspectives**, Oxford, v. 16, n. 1, p. 86-105, fev. 2015.

KNIGHT, P. T. **A Internet no Brasil:** Origens, Estrategia, Desenvolvimento e Governança. Rio de Janeiro: Self-published, 2014.

KRASNER, S. D. **International Regimes**. Ithaca: Cornell University Press, 1983.

KURBALIJA, J. **An Introduction to Internet Governance 7th Edition**. 7ª. ed. Msida: DiploFoundation, 2016.

KWALWASSER, H. Internet Governance. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. **Cyberpower and National Security**. Washington: Center for Technology & National Security Policy, 2009. Cap. 21.

LEINER, B. et al. Brief History of the Internet. **Internet Society**, 2012. Disponivel em: <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>. Acesso em: fev. 2017. Arquivo PDF.

LITMAN, J. The DNS Wars: Trademarks and the Internet Domain Name System. **Univeristy of Michigan**, 2000. Disponivel em: <http://www-personal.umich.edu/~jdlitman/papers/DNSwars.pdf>. Acesso em: mar. 2017. Arquivo PDF.

MARKOFF, J. **What the Dormouse Said:** How the Sixties Counterculture Shaped the Personal Computer Industry. London: Penguin Books, 2005.

MOCKAPETRIS, P. Request for Comments: 883. **RFC Editor**, 1983. Disponivel em: <https://www.rfc-editor.org/rfc/rfc883.txt>. Acesso em: 2018.

MOODY, G. Russia says disconnecting from the rest of the net 'out of the question', but wants alternative DNS servers for BRICS nations. **Tech Dirt**, 2017. Disponivel em: <https://www.techdirt.com/articles/20171206/03565338753/russia-says-disconnecting-rest-net-out-question-wants-alternative-dns-servers-brics-nations.shtml>. Acesso em: 2018.

MOOG, S.; SPICER, A.; BÖHM, S. The Politics of Multi-Stakeholder Initiatives: The Crisis of the Forest Stewardship Council. **Journal of Business Ethics**, Dordrecht, v. 128, n. 3, p. 469–493, mai. 2015.

MORRIS, I. Seven Ways Windows 95 Changed The World. **Forbes**, 2015. Disponivel em: <https://www.forbes.com/sites/ianmorris/2015/08/24/windows-95-changed-the-world/>. Acesso em: nov. 2017.

MUELLER, M. **Ruling the Root:** Internet Governance and the Taming of Cyberspace. Cambridge: MIT Press, 2004.

NAUGHTON, J. Netscape: the web browser that came back to haunt Microsoft. **The Guardian**, 2015. Disponivel em: <https://www.theguardian.com/global/2015/mar/22/web-browser-came-back-haunt-microsoft>. Acesso em: mar. 2017.

NOSS, E.; GOMES, C. ICANN History Project: Chuck Gomes and Elliot Noss discuss ICANN's early days [202E]. **Youtube**, 2017. Disponivel em: <https://www.youtube.com/watch?v=WN3qNja8708>. Acesso em: 2018.

PELKEY, J. Chapter 4: Arpanet: 1969-1972: The Beginnings of Computer Networks — 4.2 Host-to-Host Software: The Network Working Group 1968-1969. **Entrepreneurial Capitalism and Innovation:** A History of Computer Communications 1968-1988, nov 2007. Disponivel em: <http://www.historyofcomputercommunications.info/Book/4/4.2-Host-to-HostSoftwareTheNetworkWorkingGroup68-69.html>. Acesso em: nov. 2017.

STANDAGE, T. **The Victorian Internet:** The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers. 2ª. ed. New York City: Bloomsbury USA, 2014.

TAYLOR, E. Internationalised Domain Names: State of Play. **EURid**, 2011. Disponivel em: <https://eurid.eu/media/filer_public/f8/14/f814332f-b03d-4fa0-9c09-86f426de4550/insights_idns.pdf>. Acesso em: 2018.

TEETER, P.; SANDBERG, J. Cracking the enigma of asset bubbles with narratives. **Strategic Organization**, Thousand Oaks, v. 15, n. 1, p. 91-99, 2017.

TELEANU, S. The IANA stewardship transition: what is happening? (Part I). **Diplo**, 2016. Disponivel em: <http://www.diplomacy.edu/blog/iana-stewardship-transition-what-happening-part-i>. Acesso em: out. 2016.

THE WASHINGTON POST. Jon Postel, Internet Pioneer, Dies at 55 After Heart Surgery. **The Washington Post**, 1998. Disponivel em: <https://www.washingtonpost.com/archive/local/1998/10/18/jon-postel-internet-pioneer-dies-at-55-after-heart-surgery/75b75d28-95c1-4a6b-9a0b-2b7f08533fbc/>. Acesso em: nov. 2017.

TSEBELIS, G. **Veto Players:** How Political Institutions Work. Princeton: Princeton University Press, 2001.

VAUGHAN-NICHOLS, S. ICANN makes last minute WHOIS changes to address GDPR requirements. **ZDNet**, 2018. Disponivel em: <https://www.zdnet.com/article/icann-makes-last-minute-whois-changes-to-address-gdpr-requirements/>. Acesso em: 2018.

W3C. Montevideo Statement on the Future of Internet Cooperation. **W3C**, 2013. Disponivel em: <https://www.w3.org/2013/10/montevideo.html.en>. Acesso em: 2013 2018.

WEBER, M. The Three Types of Legitimate Rule. In: SICA, A. **Max Weber:** A Comprehensive Bibliography. New Jersey: Transaction Publishers, 2004.

WGIG. **Report of the Working Group on Internet Governance**. Nações Unidas. Tunis, p. 24. 2005.

WHEELWRIGHT, G. US to give up control of the internet's address book after years of debate. **The Guardian**, 2016. Disponivel em: <https://www.theguardian.com/technology/2016/oct/04/us-government-internet-control-iana-address-book>. Acesso em: out. 2016.

WIPO. The management of Internet Names and Aaddresses – Final report of the WIPO Internet Domain Name Process. **WIPO**, 1999. Disponivel em: <http://www.wipo.int/amc/en/processes/process1/report/finalreport.html>. Acesso em: nov. 2017.

WU, T. **Who Controls the Internet?:** Illusions of a Borderless World. Oxford: Oxford University Press, 2008.

YU, P. K. The Neverending ccTLD Story. In: WASS, E. S. **Addressing the World:** National Identity And Internet Country Code Domains. Maryland: Rowman & Littlefield Publishers, 2003. Cap. 3.