Telecommunications Policy 47 (2023) 102614

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Restraining ICANN: An analysis of OFAC sanctions and their impact on the Internet Corporation for Assigned Names and Numbers

Daniel Pérez Fernández

Universidad Autónoma de Madrid, Political Science and International Relations Department, Faculty of Law, C/ Marie Curie, N°1, Edificio de Ciencias Jurídicas, Políticas y Económicas, 1ª Planta, Ciudad Universitaria de Cantoblanco, 28049, Madrid, Spain

ARTICLE INFO

Keywords:
Domain Name System
ICANN
Lawfare
Office of Foreign Assets Control
Sanctions

ABSTRACT

The Internet Corporation for Assigned Names and Numbers (ICANN) has long played a crucial role in coordinating some aspects of the domain name system (DNS) and managing domain names and Internet Protocol Addresses. In 2016, ICANN underwent a significant transformation when completing the IANA Transition, aimed at securing the corporation's independence from U.S. government oversight. However, while the transition marked a pivotal moment in ICANN's history, the corporation still operates within U.S. jurisdiction. This situation makes ICANN subject to compliance with the U.S. Office of Foreign Assets Control (OFAC) sanctions programs, impeding the corporation from contracting and accrediting gTLD registries and registrars from countries currently targeted by OFAC, as well as individuals or entities included in OFAC's «Specially Designated Nationals and Blocked Persons» (SDN) list. This article explores the implications of the IANA Transition, the constraints that OFAC exerts on ICANN operations, and the complexities surrounding potential solutions to the OFAC sanctions quandary.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

1. Introduction

Since its creation in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) has been in charge of administering some crucial aspects of the «domain name system» (DNS), a system of rules that links Internet Protocol Addresses (IPs) with the names we are used to type every day in our web-browsers. Until 2016, ICANN performed some of its most essential duties under direct supervision by the U.S. National Telecommunications Administration (NTIA), with whom it held a contract regarding the so-called «IANA functions». Specifically, ICANN did the following because of the contract established with NTIA: (1) Coordinate the assignment of technical protocol parameters; (2) perform administrative functions associated with root management; and (3) allocate Internet Protocol address blocks to Regional Internet Registries (RIRs) for further distribution (NTIA, 2000).

As it will be covered in some depth in Sections 2 and 3 of this article, the original plan was to end NTIA's direct oversight of the «IANA functions» by 2000. However, the contract was extended for sixteen more years (Mueller, 2014:37). Reasonably, the protraction

E-mail addresses: daniel.perezf@uam.es, daniel.perezfernandez@estudiante.uam.es.

https://doi.org/10.1016/j.telpol.2023.102614
Received 28 November 2022; Received in revised form 15 July 2023; Accepted 17 July 2023
Available online 24 July 2023

of NTIA's oversight fostered lots of criticism and gave way to long, heated discussions aimed at pushing ICANN to pitch NTIA on ending its supervisory role.

In 2014, when NTIA announced it was finally backing off, many stakeholders thought ICANN would finally evolve into a full-fledged "global corporation" performing unadulterated "global governance" (vid. ICANN, 2014).[1] The removal of NTIA from ICANN operations was over-enthusiastically celebrated as synonymous with a complete divorce between the corporation and state-based governance mechanisms. Nevertheless, in 2016, when the IANA functions were transferred in full to ICANN, it became increasingly clear that the situation was not that simple.

Indeed, since ICANN remains incorporated in the United States, the corporation has to comply with the U.S. Office of Foreign Assets Control (OFAC) economic and trade sanctions programs. OFAC is part of the Department of the Treasury of the United States, and since 1950 it has been in charge of enforcing sanctions targeting a wide array of individuals, companies, and countries involved in activities deemed reprehensible by U.S. authorities (vid. Zarate, 2013).

OFAC sanctions aim at extensive blocking of the assets and contracting capabilities of persons –singular or collective– that pose any kind of threat to the U.S. regarding its national security or foreign policy, or that pursue activities that somehow endanger U.S. economic performance (OFAC, 2002). Indeed, all U.S. persons must comply with OFAC sanctions programs, "including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, [and] all U.S. incorporated entities and their foreign branches" (OFAC, 2015).

As an entity incorporated in the state of California, ICANN has to comply with OFAC sanction programs. And this has some significant implications. For starters, the corporation is prohibited from contracting and accrediting gTLD registry or registrar functions with individuals or entities included in any of the OFAC sanctions lists (ICANN, 2022a). Hence, as it will be further developed in Section 4, there is reason to posit that compliance with OFAC programs makes ICANN pretty much constrained or, at the very least, severely hampered in its ability to perform its role as a «neutral», non-aligned administrator for some crucial aspects of the DNS.

In what follows, this article begins by offering a (very) brief account of how the DNS started running and of how ICANN came to be (Sec. 2). Then, it details the process by which the NTIA ended its supervisory role over the corporation while enumerating the proposals that were set forth by some parties trying to (1) move ICANN headquarters outside of the United States; or (2) give the United Nations supervisory powers over the corporation (Sec. 3). Following, the article offers a thorough description of OFAC sanctioning efforts, analyzing how they affect ICANN and some other DNS operators (specifically, domain name registries and registrars) (Sec. 4). Lastly, this article concludes by browsing through some of the most significant proposals that have been set forth as a means of allowing ICANN to get rid of compliance with OFAC (Sec. 5).

It is important to note here that this article focuses –almost exclusively– on answering the question of how is it that OFAC sanctions programs affect ICANN. Certainly, this article offers some information about how OFAC sanctions programs affect domain name registries and registrars (see Sec. 4), and it includes some sparse notes hinting at potential investigation on the effects of OFAC sanctions programs on other DNS operators (e.g. authoritative nameserver operators, DNS hosting services, etc.). However, information about these other issues is deliberately kept at a minimum, leaving as much space as possible for discussing ICANN's role in the DNS, the distinct ways in which OFAC sanctions affect the corporation, and some proposals aimed at helping ICANN cast aside compliance with OFAC.

Ultimately, the central aim of this article is to analyze –as thoroughly as possible– the implications of OFAC sanctions on ICANN's operations and to highlight the complexities involved in finding solutions to address the challenges these sanctions pose to the corporation. As presented in Sec. 5, there are plenty of proposals aimed at helping ICANN escape OFAC's reach, four of them discussed in this article: (1) Relocating the corporation outside of the United States; (2) Subjecting the corporation to oversight by the UN or the International Telecommunication Union (ITU); (3) Letting ICANN develop its own sanctions programs in tandem with other –community-led– Internet actors; and (4) Granting ICANN "partial immunity" to U.S. laws under the International Organizations Immunities Act (IOIA) of 1945 (P.L. 79–291). Positively, by following any of these courses of action, ICANN would no longer need to comply with OFAC sanctions programs. However, each of the proposals discussed in the last part of this article presents its own set of technical complexities, legal uncertainties, and geopolitical dilemmas. For that very reason, this article contends that –currently– there is no foolproof solution to the OFAC's sanctions quandary, and that further work is needed in order to devise more sound fixes for this

[1] It has been rather frequent for ICANN to describe itself as a "global corporation" performing "global governance" (see for instance ICANN, 2006; ICANN, 2009, or ICANN, 2012c), though the meaning of these terms is decidedly contested. At least since the 1980s, globalization and international relations scholars have been trying to discern what are the features if any that differentiate «global» governance arrangements from «international» ones, but consensus has not ever been reached (vid. Rosenau & Czempiel, 1992; UNCGG, 1995; Sassen, 2007). However, conventional wisdom points out that "in contrast to international governance, global governance is characterized by the decreased salience of states and the increased involvement of nonstate actors in norm- and rule-setting processes and compliance monitoring", and that «global governance» is broader in scope than «international governance», since the former tries to tackle policy issues affecting "the global sphere", whereas the latter seems only concerned with those issues directly affecting the nation states comprising specific «international governance» arrangements (Brühl & Rittberger, 2001:2; Kacowicz, 2012:690).

particular issue.

2. A (very) brief history of the domain name system

Beginning in 1972, IP addresses were handled by *Internet pioneer* Jon Postel –supported by Joyce K. Reynolds from 1979 on[2]– and a small team constituting the Stanford-based Network Information Center (NIC). However, it was not until 1984 that the system acquired some level of maturity and started to resemble what we now regard as the DNS. Up until 1984, there was no such thing as «domain names». The system was solely composed of a list of socket numbers and host names[3] registered by Postel and Reynolds, first in a notebook and then in a publicly available registry held by the NIC (Carr, 2016:128). This schema worked for a bit, but as the system grew in size, it became clear that there was a need for a more straightforward, intuitive way of accessing endpoints in the network.

Domain names were created precisely in this conjuncture. The standard developed by Paul Mockapetris around 1983 introduced the schema we are accustomed to using when navigating cyberspace; that is, the system of correspondence by which a domain name –for instance, *sciencedirect.com*– is linked to a single IP address or to a set of them −162.159.129.81 and 162.159.130.81, for *sciencedirect.com*[4]– (Mockapetris, 1983a; Mockapetris, 1983b). This new schema made accessing endpoints much more manageable and helped escalate the nascent digital ecosystem to a new level. By the end of 1984, the Domain Name System –as we have come to know it– was fully operational, and starting in 1985, the first wave of domain registrations was taking place.

The initial offering of domain names only covered six possible «generic» extensions, all of which served for very specific purposes. For commercial organizations, there emerged the *.com* generic top-level domain (gTLD). For organizations involved in or developing networking technologies, there appeared the *.net* gTLD. For educational purposes, it was created the *.edu* extension. And for a broader array of organizations, such as NGOs or other non-profit bodies, there remained the *.org* gTLD. Of these four, the only TLD for which registration requirements remained rigid was the *.edu* extension.[5] In no time, the *.com*, *.net,* and *.org* spaces were bundled, and specific requirements were abandoned for the most part. The remaining two gTLDs were *.gov* and *.mil*: initially reserved and still only used for, respectively, U.S. federal government and military agencies.

In parallel to the introduction of these six gTLDs, the Domain Name System was also made home to Country Code Top-Level Domains (ccTLDs): i.e., two-letter extensions based on the ISO-3166-1 standard, put in place to indicate a site's relation to a country, such as *.no* for Norway, *.cn* for China, or *.za* for South Africa. This relatively stable compound of six gTLDs and an increasing number of ccTLDs –one in 1983, three in 1985, thirteen by 1986, etc.– was, as noted above, managed by Postel, Reynolds, and their team at the NIC. And as the DNS gained in size and importance, starting in 1988, some found it fitting to start referring to their work and endeavors using the term «Internet Assigned Numbers Authority» (IANA).

Functions then performed by IANA –and now performed by IANA under a contract with ICANN– included: (1) The coordination of the assignment of both Internet Protocol (IP) addresses and domain names, and (2) the administration and management of the DNS «root file». For clarification, it is essential to note here that the «root zone file» is the "authoritative file" containing the IP addresses associated with every domain and sub-domain that has been made part of the network (Palladino & Santaniello, 2021:45 ss.). As noted above, «root zone file» management is one of the IANA functions. However, a plurality of «DNS root servers» are also needed to make the system redundant and resilient. These «DNS root servers» are the ones responsible for the distribution of the information contained in the root zone file administered by IANA (Mueller, 2002:47). In 1984, Postel and his team set up the first of these «DNS root servers». But then, as the system escalated, other «DNS root servers» were created. These root servers are located in different parts of the world, though most of them remain in the United States.[6]

[2] It is almost routine to overlook the important role Joyce K. Reynolds had during the development of Internet routing and addressing. As mentioned above, Reynolds started helping Postel and the SRI team in 1979, but in October 1983, Postel delegated to Reynolds the full "responsibility for day-to-day assignment tasks" (Mueller, 2002:77). Furthermore, Reynolds acted as editor of the IETF's RFCs between 1986 and 2006. And she played a decisive role during the process of transfer of DNS management to the ICANN, supporting the corporation in performing these functions between 1998 and 2001. For more information on Reynolds' contributions, see for instance Milton Mueller's *Ruling the Root* (2002) or Jack Goldsmith and Tim Wu's *Who Controls the Internet?* (2006).

[3] A socket number is a combination of an IP address and a port number, defining a logical endpoint in a network connection. These numbers were recorded by Postel, Reynolds and the team at the NIC. Since they were hard to remember, numbers were given names (host names) in order to make connections easier.

[4] The IP addresses of sciencedirect.com are all IPv4 addresses. The successor standard to IPv4, IPv6, started being deployed in 2008, and IPv6 addresses now account for almost 40% of all IP addresses being used worldwide (see https://www.google.com/intl/en/ipv6/statistics.html). One of the main differences between IPv4 and IPv6 is that IPv4 addresses are 32-bit, whereas IPv6 are 128-bit. The former can generate a total of 4.29×10^9 single addresses, and the latter 3.4×10^{38}. As an example of IPv6 addresses let us see that, for instance, the IPv6 address of *wikipedia.org* is 2a02:ec80:600:ed1a:1, whereas its corresponding IPv4 address is 185.15.58.224.

[5] Initially, the *.edu* gTLD was meant to be used by educational organizations around the world. But in 2001 the U.S. Departments of Education and Commerce established that only postsecondary institutions accredited in the U.S. were eligible, since then, for registering a domain in the *.edu* namespace.

[6] As mentioned above, in 1984 there was just one «root server» set up by Jon Postel and his team at the NIC. Then, by 1985, three more «root servers» were made part of the system, two located in the University of Southern California and one in the U.S. Army Ballistic Research Laboratory. By 1987, the number of «root servers» increased to seven. And in 1991, it was deployed the first non-U.S. «root server», located in the Royal Institute of Technology of Stockholm. Between 1991 and 1997, some «root server» locations changed, and by 1997 the number was finally increased to thirteen (RSSAC, 2016).

Still and all, «DNS root servers» are not the only type of DNS servers that help in resolving domain name queries. In a standard DNS lookup –that is, when there is no caching in play[7]– four types of DNS servers work together to help in delivering the IP address for a specific domain to a client. These four types of DNS servers are: (1) «recursive resolvers», either responding to a client's query with cached (i.e. locally stored) data, or sending the query to a «DNS root server»; (2) «DNS root servers», acting as a 'first stop' for domain name queries, and either solving them autonomously or –if unable to do so– routing them to «TLD nameservers»; (3) «TLD nameservers», containing the information of all the domain names stationed under specific TLDs (e.g. *.com*, *.es*, *.top*, etc.) and pointing queries to an «authoritative nameserver»; finally (4) «authoritative nameservers», providing clients the IP addresses of the domain names they are trying to reach, and thus acting as the 'last stop' in a domain name query (vid. Cloudflare, 2023; Jeftovic, 2018:59 ss.).

During the period that goes from 1983 to 1991, all costs related to the DNS –and, therefore, those related to performing the IANA functions– were covered by the U.S. government via its National Science Foundation (NSF). However, in 1991, NSF decided it was no longer willing to financially support DNS administration (Mueller, 2002:110 ss.). Therefore, NSF opened a process for transferring management –and with it, the IANA functions– to a private actor that, from then on, would be in charge of administering the DNS and financially supporting it.

Since October 1, 1991, the firm in charge of administering the system and performing the IANA functions was Network Solutions Inc. (NSI),[8] a small enterprise from Herndon, Virginia. To help the firm perform its newfound functions, NSI was awarded by the National Science Foundation US$ 5 million, which was supposed to last for five years (Rutkowski, 2018). But in less than two years, NSI started complaining that the amount given was getting short. In this conjuncture, NSF negotiated an amendment with NSI, allowing it to start charging for new domain registrations and annual renewals (Malcolm, 2008:34). NSF celebrated the amendment with a sound statement: "[from now on] domain name services will not be subsidized by taxpayers" (NSF, 1995). Beginning in mid-September 1995, thus, Network Solutions started covering its operational expenses in full by charging registrants US$ 100 for new domain registrations and US$ 50 for annual renewals. As Anthony Rutkowski explains, by the time the amendment was signed, projections showed that "the exponential increase in […] domain names [registration] would within 2–3 years produce more than a million dollars a year in revenue at near 100% margins" (Rutkowski, 2018). And that is almost precisely what happened. By 1997, NSI's yearly revenues tripled. And in 1998, the firm reported an outstanding annual net profit of US$ 4.8 million (Clausing, 1999).

After these events, abundant criticism followed, pointing out that NSI was acting in a quasi-monopolistic fashion by grabbing all the profits derived from new domain registrations and renewals (Benkler, 2006:430). Therefore, many firms in the nascent Internet commercial ecosystem found it fitting to pressure the U.S. government, hoping it would break NSI's monopoly through a market liberalizing effort. Public powers acted, and between 1997 and 1998 three significant policy papers were released: The *Framework for Global Electronic Commerce* (1997), the *Green Paper on Internet Governance* (1998), and the *White Paper on Management of Internet Names and Addresses* (1998). On top of articulating "the approach of the Clinton administration to the future of [Internet] technology and the policy vision for its potential contribution to US power", these policy papers "formally charted a path from the existing Internet governance mechanisms to a future which was based on the establishment of the ICANN" (Carr, 2016:130).

Following their publication, arrangements were made to dismantle Network Solutions' monopoly. And this errand was accomplished by breaking apart functions then performed by the Herndon firm into two separate affairs: that of the «registries» and that of the «registrars». From then on, companies in the registry camp would be in charge of administering and setting the rules for the allocation of one or several gTLDs, leaving to the registrars the selling of specific domain names to users (Froomkin & Lemley, 2003:7). As such, the new system would make users pay to registrars for purchasing specific domains; and registrars would pay to registries for acquiring the rights to sell domains stationed under the TLDs managed by each registry. Notwithstanding that this arrangement still made it possible for NSI to play in both fields –as it swiftly split its registry and registrar functions into two separate branches–, the deal was a game-changer and made the system consistent with the oft-sacralized principle of competition that pervaded most U.S. officials public policy outlook for the ICT realm (vid. Carr, 2016:57).

Under these circumstances, the Internet Corporation for Assigned Names and Numbers (ICANN) entered the picture, in 1998, as a non-profit established to coordinate registry and registrar operations, and honored with performing the IANA functions. As Mark Raymond and Laura DeNardis explain, ICANN was made responsible for the "allocation of blocks of Internet numbers to regional Internet registries for further distribution", for the "oversight of the Internet's root server system operations", for "the establishment of policies for introducing new top-level domains to the root system", and for "oversight of domain name assignment" (Raymond & DeNardis, 2015:594).

Indeed, it is essential to underscore that the corporation was designed as a California-based non-profit and that it was put in place, most importantly, due to a decision ultimately made by the U.S. administration. The Internet's own technical and user community was asked for input, and other governments engaged in the process (Mueller, 2002:164). But still, it was the government of the United States who laid down the law.

As a matter of fact, between 1996 and 1998, some organizations advocated quite a different arrangement than that culminating with the creation of ICANN. The «International Ad Hoc Committee» (IAHC) –integrated, among others, by the Internet Society (ISOC), the International Telecommunication Union (ITU), the World Intellectual Property Organization (WIPO), and IANA– advocated for the creation of the «International Council of Registrars» (CORE), an organization that would have been based in Switzerland and that would have been in charge of performing the IANA functions and of coordinating registry and registrar operations (Goldsmith & Wu,

[7] Caching is the process of storing data in a cache, which is a temporary storage area that facilitates faster access, improving system performance.

[8] Almost immediately, NSI subcontracted with Jon Postel and Joyce K. Reynolds the performance of some of the functions that Postel himself, Reynolds and the team at the NIC were already carrying out prior to the arrangement between NSF and NSI (vid. Mueller, 2002:101 ss.).

2006:39). The IAHC proposal went seemingly unnoticed by the U.S. administration, and the group even set up an opening ceremony, in 1997, that would have formally set CORE in motion. Nevertheless, the United States administration finally vetoed IAHC's arrangement by announcing that IANA was subject to U.S. authority because of the contract that NSF still had with Network Solutions (NSI). Thus, no changes would be accepted in the way that IANA was managed without the approval of the U.S. administration (Goldsmith & Wu, 2006:40).

By doing this, the U.S. administration showed the organizations comprising IAHC –including IANA itself– that it was still in charge.[9] Indeed, many of the proposals that IAHC was trying to set forth –like that of breaking apart registry and registrar functions– were included by the U.S. administration in its «Green» and «White» papers from 1998 (see above). But the idea of moving IANA outside of the United States was clearly a no-go for U.S. authorities (ibid., 2006:42). Thence, the path charted by the U.S. government in the «Green» and «White» papers advocated for putting IANA in the hands of ICANN, a corporation that, as already advanced, was to be born as a non-profit incorporated in the state of California.

When ICANN was finally set up, the U.S. administration secured oversight of the IANA functions by making ICANN sign a contract with NTIA. This contract outlined the services and functions that, from then on, ICANN would provide and perform "on behalf of the U. S. government" (ICANN, 2000). Specifically, ICANN would be doing the following by way of the contract established between NTIA and the corporation: (1) "Coordinate the assignment of technical protocol parameters"; (2) "perform administrative functions associated with root management"; and (3) "allocate [Internet Protocol] address blocks" to Regional Internet Registries (RIRs)[10] for further distribution (NTIA, 2000). This arrangement was supposed to last for two years, after which NTIA would transfer to ICANN the IANA functions and stop performing its supervisory role (Mueller, 2015:3). But interestingly enough, formal supervision by NTIA lasted until October 2016.

As already advanced, and in addition to being the organization in charge of performing the IANA functions on behalf of the U.S. government, ICANN was given some other roles and capacities, like that of coordinating and administering registry and registrar operations. Thereupon, the corporation was given the power to enact its own coordination policies, and it was allowed to start requiring gTLD registries and registrars to enter into «agreements» (i.e., contracts) in which the corporation outlays the obligations these operators have to observe to start performing such functions in the DNS (vid. ICANN, 2017; 2022a; 2022b).

Since then, one of the obligations that both gTLD registries and registrars have to honor is that of economically compensating ICANN for its coordinating and administration efforts. For the regular registrar, this means giving ICANN: 1) A standalone payment of US$ 3,500 in terms of a non-refundable application fee; 2) a yearly US$ 4,000 accreditation fee due upon approval of operations and each year thereafter; 3) a variable quarterly fee based on ICANN's operating costs; and 4) a flat quarterly fee charged for each new registration, renewal or transfer of domain names (ICANN, 2012a). For gTLD registries, the arrangement is slightly different,[11] making them pay: 1) A quarterly US$ 6,250 fixed fee for accreditation purposes; 2) a variable fee based on multiplying US$ 0.25 by the total amount of new domain registrations in TLDs administered by the registry; 3) a one-time mandatory fee of US$ 5,000, in terms of access and use of the tools for intellectual property rights enforcement ICANN offers (ICANN, 2017).

Contrastingly, ccTLD operators do not have to compensate ICANN for its coordination endeavors, though most of them «voluntarily» remunerate the corporation.[12] For instance, the operators of the *.uk* and *.it* ccTLDs (ISO-3166-1 codes for the United Kingdom and Italy) vowed to give ICANN US$ 85,000 annually. And the operators of the *.ua* and *.nz* ccTLDs (i.e., codes for Ukraine and New Zealand) established that they would give the corporation US$ 15,000 *per annum*. Others, like the *.mx* –Mexico– operator, pledged to annually "contribute to ICANN's cost of operations" with US$ 25,000. And the Senegal ccTLD (*.sn*) managers thought it was adequate to pay the corporation US$ 2,000 starting in 2007.

This different treatment between, on the one hand, gTLD registries and registrars, and on the other, ccTLD operators, stems from the fact that, as noted above, ICANN is in charge of «accrediting» the former to allow them to perform such functions in the DNS. But the corporation cannot force any contractual terms upon ccTLD operators. Indeed, as put forth by Internet governance scholars Milton Mueller and Farzaneh Badiei, the rationale for this disparate treatment is relatively straightforward, and it derives from the glaring difference made by ICANN between gTLD and ccTLD operations: "gTLDs are heavily regulated by ICANN contracts, they are subject to ICANN policy-making processes, and [its operators] pay fees to ICANN. ccTLDs [operators], on the other hand, do not [...] have contracts with ICANN and make only voluntary contributions to the support of the corporation" (Mueller & Badiei, 2017:446).

[9] The idea that the U.S. administration was «still in charge» wasn't as readily or equally accepted by all the organizations and individuals comprising the IAHC. For instance, Jon Postel refused to acknowledge U.S. authority, and after the IAHC and CORE proposals were struck down, he asked root servers operators to recognize his computer as the one in charge of managing the «root zone file». As a consequence, during almost a week, eight of the thirteen root servers pointed to Postel's computer for validation, while the other five recognized NSI as the «root zone file» manager (Goldsmith & Wu, 2006:45–46). After the U.S. administration noticed the split, it politely asked Postel to stop messing around, or else face criminal charges.

[10] Currently, there are five Regional Internet Registries (RIRs) in operation: (1) AFRNIC, distributing IP addresses in Africa; (2) ARIN, serving Canada, the United States, Antarctica and some parts of the Caribbean; (3) APNIC, in charge of Oceania and East and South Asia; (4) LACNIC, serving South and Central America and most of the Caribbean; and (5) RIPE NCC, distributing numbering resources in Europe, Greenland and West, Central and North Asia. As mentioned above, RIRs are allocated IP addresses by IANA, and then they distribute those addresses to Internet Service Providers (ISPs) and/or end-user organizations located in the regions in which each of them operates.

[11] The information provided in the paragraph is extracted from ICANN's *Base Registry Agreement*, as updated 31 July 2017. This document is the benchmark work from which all gTLD Registry Agreements (RAs) are derived, though gTLD registries can –and often do– negotiate with ICANN some adjustments to their singular RAs.

[12] All ccTLD agreements are available entering: https://www.icann.org/resources/pages/cctlds/cctlds-en.

\

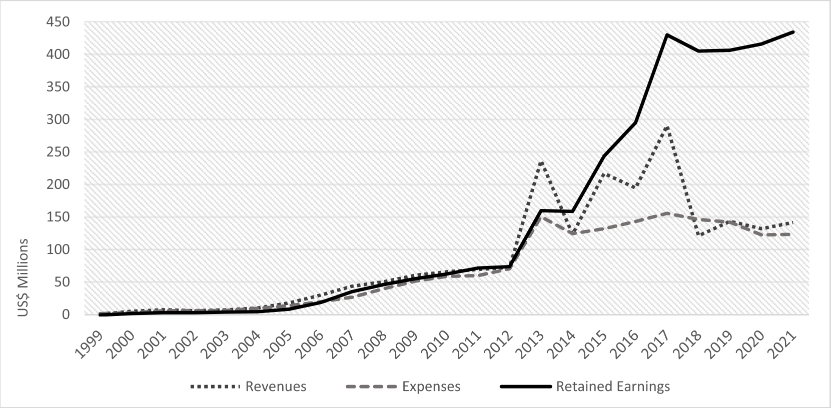

Fig. 1. ICANN's yearly revenues, expenses, and retained earnings (1999–2021) [13].

Being able to collect fees from both gTLD registries and registrars (and, on a voluntary basis, from ccTLD operators), ICANN's financials slowly increased since its creation, though its revenues barely covered its operational expenses between 1999 and 2012. Nevertheless –as shown below, in Fig. 1– ICANN's financial situation improved from 2012 on, as the corporation started deploying its «New-gTLD Program». This program, run between 2012 and 2017, consisted in the expansion of the array of gTLDs included in the DNS.

It seems on point to recall here that since the DNS was created and until 2012, the number of TLDs made part of the DNS was somewhat limited. From 1983 on, users could register a name only in the six original gTLDs or in the ccTLDs that were progressively included in the DNS. Then, in 2000, ICANN created the *.aero*, *.biz*, *.coop*, *.info*, *.museum*, *.name,* and *.jobs* gTLDs. And later on, in 2004, the corporation included the *.asia*, *.cat*, *.jobs*, *.mobi*, *.post*, *.tel,* and *.travel* general extensions. The number of gTLDs available in 2004 was, thus, situated at twenty. But then, with the deployment of the «New-gTLD Program», the corporation created more than 1,200 new gTLDs, the most famous of which are *.app*, *.club*, *.icu*, *.online*, *.site*, *.shop*, *.top*, *.vip*, *.work* or *.xyz.*[14]

Positively, the «New-gTLD Program» helped ICANN transform its financial situation from *barely sustainable* to *vigorous* (see Fig. 1). As a result of this gargantuan expansion of the number of gTLDs, ICANN secured many contracts that, especially between 2012 and 2017, helped the corporation boost its yearly earnings. Though as noted above, the program was terminated in 2017. Ever since then, ICANN's revenues and expenses have settled in around US$ 120–150 million per year, and its retained earnings now amount to circa US$ 429 million (that is, almost six times what the corporation had in 2012 and a hundred times what it owned in 2004).

To adequately perform the various functions ICANN was entrusted with in 1998, the corporation was soon required to develop a complex organizational structure. Thus, ICANN was rapidly organized into three pillars: (1) The «Board of Directors» of the corporation; (2) The «ICANN Community», comprising three Supporting Organizations (SOs) and four Advisory Committees (ACs); and (3) the corporation's «Staff». As explained by ICANN itself, "the Community [SOs and ACs] develop and influence [the corporation's] policies through their input, discussion, and advocacy for their point of view. [The] Board reviews the policy development outcomes and makes final decisions whether to approve or reject them. [And ICANN] Staff provide the Community [SOs and ACs] with administrative and substantive support in the policy development, and ultimately implements Board approved policies" (ICANN, see note below [15]).

Specifically, the three «Supporting Organizations» (SOs) that are part of ICANN's Community are: (1) The Generic Names Supporting Organization (GNSO), in charge of developing policies for gTLDs; (2) The Country Code Names Supporting Organization (ccNSO), accredited with doing the same as GNSO but for ccTLDs; and (3) The Address Supporting Organization (ASO), which develops policies on IP addresses and oversees the allocation of these numbering resources by Regional Internet Registries (RIRs). Then, the four «Advisory Committees» (ACs) comprising ICANN's Community are: (1) The At-Large Advisory Committee (ALAC), which provides advice on various ICANN activities as they relate to the interests of individual Internet users; (2) The Governmental Advisory Committee (GAC), comprised of national governments' representatives and focused on providing ICANN advice on policies that might interfere or collide with national laws or international agreements; (3) The Security & Stability Advisory Committee (SSAC), centered in providing ICANN important advice in all things related to the technical operation of the Internet's naming and addressing system;

[13] Self-made using data retrieved from ICANN's externally audited annual financial reports, available at https://www.icann.org/resources/pages/governance/current-en. The chart does not include net capital assets in ICANN's possession –which in 2021 amounted to US$ 15,231,000– or investments from which the corporation could obtain additional revenues.

[14] These ten «new» gTLDs are the ones with more names registered in 2023. Statistics for new TLDs use can be found both at https://ntldstats.com/tld and https://domainnamestat.com/statistics/tldtype/new.

[15] Information about ICANN's organizational structure is available at: https://atlarge.icann.org/about/how-is-icann-organized.

and (4) The Root Server System Advisory Committee (RSSAC), doing almost the same as SSAC, but in all things related to the technical operation of the Internet's root server system.

The main difference between SOs and ACs is that the former are responsible for developing policies for the three thematic areas conventionally linked to ICANN –gTLDs, ccTLDs, and numbering resources–, while the latter are only authorized to give advice to SOs and the Board. Nevertheless, this does not mean that ACs remain powerless. The two «technical» ACs –SSAC and RSSAC– are essential to the DNS functioning, and their advice is roughly always heeded –if not directly sought– by all three SOs and the Board. Then, the «non-technical» (sometimes called «political») ACs, GAC and ALAC, have seen some significant disparities in terms of the weight that has been given to their advice, both by SOs and the Board. Indeed, both ACs are allowed to make recommendations. But input from the GAC is almost always noted, while advice from ALAC has often been ignored (vid. De Vey & Rijgersberg, 2015:167). However, changes introduced to the corporation's organizational structure in 2016 now give ALAC a much more significant role, situating it –almost– on par with the GAC.[16]

3. Ending NTIA's oversight: the IANA transition

As mentioned in the previous section, NTIA's contract with ICANN regarding the IANA functions was initially meant to expire around 2000 but was extended for sixteen more years. This extension of the contract's original terms led to long, heated discussions on how to end U.S. oversight (Cogburn et al., 2005; Kleinwächter, 2009). As addressed by Mueller, zeal over this matter reached its first peak during the World Summit on Information Society (WSIS) –"an emphatically multilateral, state-centric series of diplomatic conferences held from 2002 to 2005 that attempted to address the whole range of relevant issues related to the information society" (Mueller, 2010:10)– and permeated the recommendations that the United Nations Working Group on Internet Governance (WGIG) made after WSIS concluded.

By and by, this group proposed four alternative models with which to address the plight of how to end U.S. oversight. In three of them, the WGIG proposed creating an «Internet Council» that would replace the U.S. administration in performing its supervisory role (WGIG, 2005). Only the fourth "indicated that there [was] no need for an oversight organization" (Drake, 2016:20). Still, at this point, none of them prevailed, because the U.S. government refused to give up its supervisory role. In a public letter issued in 2005, NTIA claimed that it would "continue to provide oversight so that ICANN maintains its focus and meets its core technical mission" (NTIA, 2005).

During this period, most concerns about U.S. oversight of ICANN operations were raised by national government representatives –like those of Brazil, India, China, and Russia– in forums such as WSIS, but also as part of routine discussions held by ICANN's own Governmental Advisory Committee (GAC). During these discussions, some GAC members indicated that since the U.S. administration was supervising ICANN, there was a clear risk that it could impinge on or meddle with specific policies developed by the corporation (Lipscy, 2017, Ch.7). To support such claims, GAC members tended to recur to the example of two «major» incidents involving U.S. interference. The first of these «major» incidents happened in 2005, when the U.S. administration forced ICANN to reopen the bidding process for the *.net* gTLD after the corporation had already awarded Verisign the registry contract to operate it. The second, in turn, developed between 2000 and 2011, and consisted in a continued blocking by U.S. authorities of the deployment of the *.xxx* gTLD, aimed at domains hosting adult-only content (vid. U.S. Congress, 2006; Mueller, 2010:71–73).

These two «major» incidents –and some similar ones[17]– were used to exemplify the dangers of U.S. oversight of ICANN operations. Nevertheless, cautioning against such dangers remained flimsy until 2013. Undeniably, it was only in the aftermath of Edward Snowden's 2013 revelations about the massive surveillance programs conducted by the United States National Security Agency (NSA) that NTIA's oversight began to be seriously questioned (vid. Mueller, 2014; Raustiala, 2016). After Snowden disclosed information about the NSA surveillance programs, most stakeholders –and not only GAC members– started thinking the time was ripe for severing ICANN's ties with the U.S. administration. As Samantha Bradshaw and Laura DeNardis explain, "concern about National Security Agency (NSA) surveillance practices […] created a loss of trust in the stewardship of the U.S. government" (Bradshaw & DeNardis, 2016:9). Similarly, Derrick Cogburn posits that such widespread and large-scale surveillance practices undermined "the trust of the global community [regarding the United States] role as a caretaker of the Internet" (Cogburn, 2017:20).

Even though NSA's surveillance practices had little to do with ICANN and the DNS, distrust of the U.S. quickly percolated all instances and levels of Internet governance. Hence, the ICANN «Community» found it fitting to pressure the Board to take the

[16] As noted by a number of commentators, since becoming part of the ICANN «Community», ALAC and GAC sought to expand their influence, wanting to become 'constituent bodies' in ICANN's organization rather than remain advisory committees (see for instance Casey, 2008; Kesan & Gallo, 2008). However, ICANN reforms progressively gave GAC more weight while leaving ALAC in pretty much the same position as it originally was. As explained in Sec. 3 of this article, changes introduced into ICANN's organizational structure in 2016 now situate ALAC almost on par with the GAC, and both ACs currently hold roughly the same power as ICANN SOs (vid. Palladino & Santaniello, 2021). Indeed, both committees remain formally chartered as ACs, but for practical purposes they are now almost equal to SOs. Contrastingly, SSAC and RSSAC have not ever craved becoming 'constituent bodies' in ICANN's organization or to forcibly expand their powers.

[17] There were, indeed, some other noteworthy incidents happening between 1999 and 2013. For instance, in 2001, the U.S. administration required ICANN to redelegate management of the *.us* TLD to Neustar, even though the corporation had already delegated this ccTLD to Verisign. And in 2006, it forced ICANN to renew the *.com* gTLD contract with Verisign, vitiating the process for contract renewal that the corporation had established. Then, in 2012, during the first phase of the New-gTLD Program, the U.S. administration made ICANN include extensive «background checks» on new gTLD registry applicants, citing concerns about the possibility that new gTLDs could end up being controlled by «untrustworthy organizations».

necessary steps to detach the corporation from U.S. oversight (Mueller, 2014:40 ss.). The Board reacted, and ICANN's CEO at the time, Fadi Chehadé, took the lead by signing the *Montevideo Statement on the Future of Internet Cooperation*: a manifesto in which the heads of the leading Internet institutions expressed a "strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance" (ICANN, 2013a).[18] On top of denouncing this situation, signatories of the *Montevideo Statement* went a step further, calling "for accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing" (ibid., 2013).

A few months after signing the *Montevideo Statement*, organizations such as the Internet Society (ISOC), the Internet Engineering Task Force (IETF), and ICANN itself started pitching the U.S. administration on the possibility of fully transferring the IANA functions to ICANN. This design was christened the «IANA Stewardship Transition», and with it, oversight enforced by NTIA on the IANA functions was intended to come to an end. The ICANN–ISOC–IETF proposal emphasized the importance of a bottom-up, consensus-based approach to managing the DNS, and sought to ensure that the DNS remained a global public resource that was not subject to undue government control or interference (Palladino & Santaniello, 2021:71 ss.). The proposal aimed at ending U.S. oversight was officially sent to NTIA in March 2014. And quite swiftly after that, the U.S. National Telecommunications Administration agreed to start the process of detaching itself from the IANA functions.

The «IANA Stewardship Transition» started in the final days of March 2014 and ended on October 1, 2016. During the interim, and before the transition was formally set in motion, some of the national governments that took the lead during the WSIS negotiations saw an opportunity to subject the now-almost-independent ICANN to scrutiny by the UN or some other intergovernmental body, while some others pushed for moving the corporation's headquarters outside of the United States.[19] For instance, representatives from the Russian and Chinese administrations advocated for transferring all of ICANN's functions to the UN's International Telecommunication Union (ITU) (Cavalli & Scholte, 2021; Negro, 2019; Stadnik, 2021). And the Brazilian government pushed for reinforcing ITU *vis-à-vis* ICANN and, later, for bolstering the presence and power of GAC's representatives inside the corporation (Kovacs et al., 2014; Trinkunas & Wallace, 2015)[20]. Further on, some parts of the Argentinian and Iranian administrations claimed it would be a good idea to move ICANN's headquarters outside of the U.S. (Corwin, 2016). And a compound of civil society associations primarily based in India defended splitting up the corporation into different organizations and then dispersing the resulting organizations along different jurisdictions (Prakash, 2016).

However, none of these proposals were even slightly considered during the «IANA Stewardship Transition». NTIA formally opened the process by stating that it would "not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution", and by asserting that ICANN would remain headquartered in the United States (NTIA, 2014; IANA-STCG, 2016). Both these provisions made it clear that NTIA aimed to trust ICANN with the IANA functions without altering much else. Therefore, parties trying to introduce more drastic changes in the way the DNS was managed –as the ones mentioned above– saw their expectations thwarted.

Contrastingly, some parties saw the transition as going too far. For instance, U.S. Senator Ted Cruz and Representative Sean Duffy –supported by a big group of other Republican Lawmakers[21]– opposed the «IANA Stewardship Transition» on grounds that it would create an "oversight vacuum" regarding the IANA functions that would be used by "rival countries" (i.e., China, Russia, Iran, etc.) to further their "authoritarian" Internet governance agendas (vid. Kleinwachter, 2016). Sen. Cruz and Rep. Duffy subsequently tried to block the transition by presenting both in Senate and in the House of Representatives the *Protecting Internet Freedom Act* (S.3034/H.R.5418), aimed at "prohibit[ing] the National Telecommunications and Information Administration from allowing the Internet Assigned Numbers Authority functions contract to lapse unless specifically authorized to do so by an Act of Congress" (U.S. Congress, 2016a,b).[22] Cruz and Duffy's legislative actions were endorsed by conservative organizations such as the Heritage Foundation,

[18] The *Montevideo Statement on the Future of Internet Cooperation* was signed on October 7, 2013, by Fadi Chehadé, President and CEO of ICANN at the time, but also by the heads of the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the World Wide Web Consortium (W3C) and all five Regional Internet Registries (RIRs).

[19] Proposals aimed at transferring ICANN's functions to the ITU, putting the UN on top of the corporation, or urging to move ICANN's headquarters outside of the United States, were already put forth during the WSIS negotiations (2002–2005). In 2007, the European Union also proposed to move ICANN's headquarters to a «neutral location» outside the United States, arguing that this would increase the corporation's legitimacy and credibility, helping it better perform its role as a global and neutral coordinator of the DNS.

[20] Opposition to proposals either aiming at putting the UN/ITU on top of ICANN, or willing to bolster the presence and power of GAC representatives inside the corporation, made the case that these changes would transform ICANN into an «international organization» very much smothered by «international governance» procedures (CDT, 2016; Mueller, 2015). For clarification, it is important to note here that in «international governance» arrangements all decisions are made by or at least require the approval of nation-states conforming those very governance arrangements (vid. Held & McGrew, 2000). And, certainly, if approved, any of the aforementioned proposals would have dramatically changed the way policy is developed inside of ICANN. As mentioned by Mueller, the imposition of an «international governance» framework would have altered ICANN's policy development process by impeding ICANN's Board from autonomously deciding on the approval or rejection of policies developed by ICANN's SOs (GNSO, ccNSO and ASO), instead putting that decision on the hands of the nation-states that are part of the UN, ITU, or that have a seat at ICANN's GAC (Mueller, 2015; see also De Vey & Rijgersberg, 2006).

[21] Republican lawmakers opposing the «IANA Stewardship Transition» included Senators Ted Cruz, Marco Rubio and James Lankford; and Representatives Sean Duffy, Mike Kelly, Marsha Blackburn, Greg Walden, John Shimkus, Bob Goodlatte, Darrell Issa, Doug Collins, Blake Farenthold, Ted Poe, Pete Olson, Louie Gohmert and Randy Weber.

[22] Rep. Mike Kelly presented in the House of Representatives two earlier drafts of the bill then named *Defending Internet Freedom Act* in November 2014 and in May 2015 (U.S. Congress, 2014, 2015). Needless to say, Representative Kelly's bill was rejected by Congress.

Americans for Tax Reform, and the Eagle Forum, naming a "great concern over U.S. national security" if the transition was to proceed as planned by NTIA (CEI, 2016; Neylon, 2016).

Though Sen. Cruz and Rep. Duffy's actions helped in delaying the transition, the process of transferring ICANN full control of the IANA functions was finally completed on October 1, 2016 (ICANN, 2016a). Thus, from then on, ICANN would no longer need to ask NTIA for approval when introducing changes to the DNS «root zone file» or when coordinating the assignment of technical Internet protocol parameters. The milepost was enthusiastically celebrated by many organizations and individuals, first commending "NTIA for its trust and confidence in the […] Internet community", and also by pointing out that the transition realized the DNS "management formula" that was envisioned by most of ICANN's stakeholders in 1998 (ibid. 2016a; ISOC, 2016).

On top of serving to end NTIA's oversight of the IANA functions, the transition was also helpful for introducing some far-reaching changes in how ICANN was organized. During the transition, starting in December 2014, the corporation's SOs and ACs were asked to build a «Cross-Community Working Group» (CCWG-ACCT) aimed at evaluating and proposing some courses of action with which to improve ICANN's functioning and make sure the corporation's «Board» was accountable to all of ICANN's stakeholders. Thus, the CCWG-ACCT "was chartered to consider any necessary updates to ICANN's accountability mechanisms in support of the IANA transition", and to devise some ways to make the corporation more proficient in performing its role as the administrator of some crucial aspects of the DNS (Drazek et al., 2022). Nevertheless, the magnitude of the task made it immediately clear to the «Community» that the CCWG-ACCT would need to be divided into two separate tracks: "Work Stream 1 for deliverables required prior to the IANA transition, and Work Stream 2 for items that could be finalized and implemented after the transition" (ibid., 2022).

Most of the proposals developed by the CCWG-ACCT «Work Stream 1» (WS1) were accepted by ICANN's Board on March 10, 2016, and they were made operational once the transition was completed. Among these, one of the most significant changes introduced by WS1 was the creation of an independent non-profit association named the «Empowered Community» (EC), agglutinating all three ICANN SOs and two of the corporations' ACs (i.e., ALAC and the GAC), and chartered with monitoring the «Board» and with making it accountable to all of ICANN's stakeholders (Palladino & Santaniello, 2021:129 ss.). Starting October 1, 2016, and as requested by WS1, the «Empowered Community» is currently qualified to: (1) Appoint or remove individual ICANN Board Directors (other than the President); (2) recall the entire Board if needed; (3) reject the corporation's operating plans, strategic plans, and budgets; (4) introduce changes to ICANN's Bylaws; and (5) require the Board to review and reconsider its decisions as they relate to the IANA functions.

The second track of the CCWG-ACCT, «Work Stream 2» (WS2), started running on June 2016, and it developed a *Final Report* with recommendations to ICANN two years after convening for the first time, on June 2018 (CCWG-ACCT-WS2, 2018). WS2 was primarily aimed at widening and supplementing the accountability mechanisms put in place by WS1. Nevertheless, it also focused on studying and supplying ICANN with recommendations on other decisive matters that could not be tackled during the IANA transition.

Doubtless to say, the most wrangling topic covered by WS2 was the one concerning the investigation of the effects of U.S. «legal jurisdiction» over the corporation (vid. CCWG-ACCT-WS2, 2018: Annex 4.3). As mentioned above, during the IANA transition, NTIA blocked all proposals either intending to move ICANN's headquarters outside of the U.S. or aiming at replacing NTIA's oversight with oversight from an intergovernmental organization. Thus, when the IANA transition was completed, the corporation remained headquartered in California, now removed from NTIA's direct control but still very much under the aegis of U.S. jurisdiction.

4. The impact of OFAC sanctions on ICANN

As the WS2 subgroup in charge of investigating the topic of «jurisdiction» was quick to notice, one of the most pressing issues affecting ICANN's operations was the one relating to the sanctions programs developed and enforced by the U.S. Office of Foreign Assets Control (OFAC). Certainly, the subgroup identified other areas of concern, including that of how to make ICANN able to comply with contrasting data and consumer protection laws and with distinct intellectual property regulations being applied in different jurisdictions (Drazek et al., 2022). But none of these issues seemed as pressing and far-reaching as the one regarding OFAC. Indeed, the «jurisdiction» subgroup contributions to the June 2018 CCWG-ACCT-WS2 *Final Report* were almost exclusively focused on how to better deal with OFAC sanctions programs, issuing a list of recommendations that ICANN should follow to mitigate some of the most damaging impacts these sanctions programs have had over the DNS (CCWG-ACCT-WS2, 2018:22 ss.). The «jurisdiction» subgroup recommendations regarding OFAC sanctions will be covered in depth in the next section of this article. Nevertheless, to understand these recommendations' strengths and limitations, it is first indispensable to grasp what OFAC sanctions are all about.

As already mentioned in the introduction, the U.S. Office of Foreign Assets Control (OFAC) is one of the leading U.S. agencies administering and enforcing economic and trade sanctions. If found to be involved in activities deemed reprehensible by U.S. standards, OFAC has the right to include individuals, companies, or political regimes in its sanction programs. The office started running in 1950, and, since the 2001 al-Qaeda attacks on U.S. soil, it gained traction as a tool aimed at financially choking "America's enemies" (Zarate, 2013:2). Before these events, OFAC sanctions were used, for instance, to block Chinese and North Korean assets under U.S. jurisdiction during the Korea War, to economically strangle the Cuban regime starting 1962, to block some property of the government of Iran after the hostage crisis of 1979, to pressure Serbia to end hostilities towards Croatia and Bosnia between 1993 and 1995, or to freeze abundant assets from Colombian narcotraffickers during the 90s (OFAC, 2006; Zarate, 2013).

By routinely performing such actions, OFAC showed the world the U.S. could use –and would use– other measures besides military browbeating to push individuals and regimes into abandoning any activity that could come to be viewed as a threat "to the foreign policy or national security goals" of the U.S. (OFAC, 2002).[23] And ever since the 90s, OFAC sanctions –and the variety of its targets– have all but ebbed. For starters, after 9/11, OFAC took a leading role during the «War on Terror» by freezing all assets linked to al-Qaeda and the Taliban and by financially asphyxiating the governments of Afghanistan and Iraq (Zarate, 2013). And during the past two decades, it initiated operations aimed at sanctioning the political regimes –and some shady organizations as well as individuals– in Belarus, Burma, the Central African Republic, China, the Democratic Republic of the Congo, Ethiopia, Iran, Lebanon, Libya, Mali, Nicaragua, North Korea, Russia, Somalia, Sudan, Syria, Venezuela, Yemen or Zimbabwe.[24]

OFAC sanctions can be divided into a «primary» and a «secondary» type. Primary sanctions apply only to entities under U.S. jurisdiction: "If OFAC believes such an entity [has] transacted with sanctioned entities, it may be fined by OFAC or criminally prosecuted by the Department of Justice". Secondary sanctions, on the other hand, punish third parties who have transacted with sanctions targets "but are neither subject to U.S. jurisdiction nor doing business" through U.S.-based institutions (Kessler, 2022:9).

Therefore, «primary» sanctions are the most straightforward way in which OFAC ensures that individuals and entities follow its instructions. Indeed, all U.S. persons must comply with its sanction programs, "including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, [and] all U.S. incorporated entities and their foreign branches" (OFAC, 2015). So, if found to be willfully transacting with a party included in any of OFAC lists, U.S. persons can be subject to "fines up to [US]$1 million and/or prison terms up to 20 years per violation" (Boyle, 2021:10). And, if found to be «accidently» doing business with any of them –that is, without previous knowledge that any such an individual or entity was included in OFAC sanctions lists– U.S. persons can face fines of up to US$ 311,562 or of "twice the value of the illegal transaction" (ibid. 2021:10).

This first type of sanctions is relatively clear about (1) the type of behavior that can lead to fines and/or imprisonment; and (2) the rubric of persons that must follow them. However, all of this is absent in so-called «secondary» sanctions. First, since there is no way to know for sure what types of behavior might lead OFAC to consider that there has been an infringement of its rulings (vid. Geranmayeh & Lafont, 2019; Lohmann, 2019). And second, as the rubric of persons that have to follow them is so wide-ranging as to comprise all of humanity. Since "secondary sanctions target non-U.S. individuals and entities that engage in transactions involving a U.S. sanctions target", any person –regardless of its place of operation– might face adverse consequences for transacting with individuals or entities included in OFAC lists (Portela, 2021:2). Consequences for doing so range from exclusion from operating ever again in U.S. markets, to the denial of using the US$ in international transactions and, even, facing criminal charges in the United States (Meyer, 2009; Rathbone & Egan, 2017).

To avoid punishment, U.S. and non-U.S. persons are encouraged to check the full lineup of individuals and entities currently targeted by OFAC by entering the Department of the Treasury website. OFAC regularly updates its «Specially Designated Nationals and Blocked Persons» (SDN) list and country-specific lists, including or removing entries. In OFAC's jargon, the SDN acronym stands for "individuals, groups, and entities, such as terrorists and narcotic traffickers designated under programs that are not country specific" (OFAC, 2022a). Hence, all parties must be sure they have read the SDN and country-specific lists to fend off potential sanctions.

Since ICANN is incorporated in the U.S., not complying with OFAC directives would make the corporation subject to primary sanctions. Therefore, ICANN clarifies that it will not provide most of its services to individuals or entities included in any OFAC sanction lists. "ICANN is prohibited from providing most goods or services to residents of sanctioned countries or their governmental entities or to SDNs without an applicable U.S. government authorization or exception" (ICANN, 2012b; 2022a).

Specifically, ICANN mentions such a prohibition in its New-gTLD «Base Registry Agreement» and in its «Registrar Accreditation Application Form», thus discouraging applicants from sanctioned countries –or individuals and entities marked as SDNs– from trying to reach the corporation to start performing any of those functions (vid. ICANN, 2017; 2022a). Indeed, this situation has provided a landscape in which sanctioned countries hold almost no accredited registry or registrar entities other than those managing their ccTLDs. Save for China and Russia –which respectively have 32 accredited registries and 108 registrars (CN), and 5 registries and 11 registrars (RU) located under their jurisdiction– no country targeted by OFAC seemingly has, as of today, any relevant presence in the

[23] Certainly, the U.S. has combined in many cases the issuing of OFAC sanctions with the deployment or use of its armed forces. For instance, during the Korea War, the U.S. deployed around 1,789,000 soldiers in the Korean peninsula. And during the Bosnian War, the U.S. military took the lead with Operation Deliberate Force, the massive NATO airstrikes campaign that crippled the Serbian military apparatus in Bosnia. This hybrid approach, based in combining the direct use of force and the imposition of economic sanctions, has been, in fact, rather common for the U.S. (vid. Davis & Ness, 2022).

[24] A comprehensive list including all active OFAC sanctions programs is available at https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.

registry and registrar departments.[25]

It is important to underscore here that prohibitions related to OFAC only affect ICANN's capacity to contract and accredit registries and registrars for gTLDs. As noted in Section 2, ICANN has no contractual relationship with ccTLD operators and has never had to accredit them. The corporation simply delegates ccTLDs to operators, and if a redelegation occurs, ICANN only records the new situation in IANA's «root zone file». Thus, OFAC prohibitions, as they constrain ICANN, cannot –and do not– affect ccTLD operations. They just put the corporation in a tight spot regarding the contracting and accreditation of gTLD registries and registrars.

Withal, OFAC can decide on issuing authorizations that ICANN can use to contract gTLD operations with entities included in country-specific lists. Specifically, OFAC does this (1) by granting a «General License» covering all individuals and entities affected by country-specific sanctions programs; or (2) by issuing «exclusive authorizations» to specific OFAC targets by request of ICANN. To secure one of these «exclusive authorizations», ICANN has to provide OFAC with detailed information on why a specific deal poses no danger or risk to the United States (Badiei, 2017). «General Licenses», on the other hand, are provided by OFAC on its own initiative when the U.S. Department of the Treasury thinks that certain deals should get an exemption from the general sanctioning provisions contained in OFAC's country-specific programs (CHE Project, 2013; vid. OFAC, 2023).

Until now, OFAC has only extended two country-specific «General Licenses» allowing ICANN to contract gTLD registry and registrar functions to entities from sanctioned countries. The first one, handed out by the Department of the Treasury in 2019, made it possible for ICANN to contract Venezuelan entities to perform these functions (OFAC, 2019). And the second, issued in 2022, re-allowed the corporation to contract and accredit Russian entities (OFAC, 2022b). However, these are the only two instances in which OFAC decided to exempt these services from its country-specific sanctions programs.

For its part, ICANN has sought «exclusive authorizations» on behalf of sanctions targets an indeterminate number of times. Information about petitions made by ICANN to OFAC is kept confidential, since ICANN lists these arrangements as qualifying for "nondisclosure" under its self-imposed «Documentary Information Disclosure Policy» (DIDP) (ICANN, 2023). Therefore, measuring how often the corporation reached OFAC trying to secure an «exclusive authorization» is problematic. And it is even more problematic knowing how many of these petitions came to fruition. Still and all, the corporation takes pride that it "has sought and been granted [authorizations] as required" (ICANN, 2017; 2022a). Though, as noted above, it seems nearly impossible to survey how often this has actually happened.

Besides ICANN itself, registries and registrars located in the U.S. are also required to comply with OFAC sanctions programs.[26] And this means that, like ICANN, they are prohibited from conducting any business with individuals or entities included in its lists. Indeed, «primary sanctions» can be applied to U.S.-based registries and registrars if they deal with SDNs or country-specific sanctions targets. And OFAC can also seize domains administered, or handed out by these registries and registrars, if the registrant of any such domains is a target of sanctions.

Positively, during the past two decades, OFAC has consistently used its power for seizing domain names. For instance, in 2008, it seized 80 domains from a travel agent offering trips to Cuba pursuant to multiple OFAC sanctions being applied to the Caribbean island (Liptak, 2008). Then, in 2013, it seized more than 700 domains allegedly linked to the –by all means malicious– Syrian Electronic Army (Krebs, 2013). And lastly, between 2020 and 2021, it seized around 120 domains that belonged to either Iranians or Iraqis under the pretext that they were linked to the Islamic Revolutionary Guard Corps (IRGC) or Hezbollah (U.S. Department of Justice, 2020, 2021).

Extensive work has shown that some of these domains were, indeed, linked to the Syrian Electronic Army, the IRGC, or Hezbollah. But others were media outlets or personal blogs hardly linked to any of these OFAC-targeted groups (Committee to Protect Journalists, 2021). However, all domain names seized in these operations were registered under the *.com*, *.org*, or *.net* gTLDs: three of the most important «legacy» gTLDs, and three gTLDs administered by U.S.-based registries.[27] Therefore, under the rules established by OFAC itself, these operations were justifiable and valid.

[25] According to ICANN's Accredited Registrar and Registry Listings (available at https://perma.cc/LR9S-BUW8 and https://perma.cc/ZX9Q-DCH5), there seems to be no single accredited registry or registrar located in Afghanistan, the Central African Republic, Cuba, the Democratic Republic of the Congo, Ethiopia, Iran, Lebanon, Libya, Mali, Nicaragua, North Korea, Somalia, Sudan, Syria, Venezuela, Yemen or Zimbabwe. There is one accredited registry and one accredited registrar located in Iraq; and there is one accredited registrar located in Belarus. However, these listings are partial and incomplete. Some operating registries and registrars are currently not included in ICANN's lists. And these lists do not include «resellers» (i.e. companies that offer domain name registration services without being required to accredit themselves through ICANN). Thus, there is reason to believe that even if ICANN's listings indicate that there are little to no registry or registrar services located in countries heavily targeted by OFAC, there might be some registries and registrars operating from these countries but not included in the corporation's lists. Plus, there could be plenty of «resellers» located in heavily targeted countries that may be providing registration services to nationals from these countries (for more information on resellers operations, see ICANN, 2013b).

[26] Certainly, U.S. registries and registrars are not the only U.S.-based DNS companies required to comply with OFAC sanctions programs, since, as noted above, all U.S. persons must comply with them (OFAC, 2015). This means that, *inter alia*, U.S. companies providing services for resolving of DNS queries like «authoritative nameservers» administrators (see Sec. 1) or DNS hosting services, are bound to OFAC's directives as much as ICANN and registries and registrars are. Indeed, during the last couple of years, some of these companies have suspended or even cancelled services for clients included in OFAC countryspecific lists or marked as SDNs. For instance, one well-known «authoritative nameserver» administrator, Cloudflare, started suspending services to OFAC targets in July 2019 after publicly recognizing that it had avoided complying with OFAC sanctions programs for a long time (vid. Sun, 2019; Cloudflare, 2022).

[27] Verisign, a company located in Reston, Virginia, has been acting as registry for the *.com* and *.net* TLDs since 2000. It also managed the *.org* namespace between 2000 and 2003. In 2003, the non-profit organization Public Internet Registry (PIR), backed by the Internet Society, took over the *.org* registry functions and has been managing this namespace ever since then. PIR is also based in Reston, Virginia.

Indeed, in these operations, OFAC had the option of seizing domain names because they were placed in gTLDs administered by registries located in the United States. But, as mentioned above, OFAC can also seize domain names if they have been handed out to registrants by U.S.-based registrars (vid. Badiei, 2017). However, there is no proof that OFAC ever approached U.S.-based registrars with seizure warrants.

As already noted, entities operating outside the U.S. can also be subject to «secondary» sanctions. And this means that, for example, registries and registrars operating from places as distinct as the EU, Russia, Argentina, or Taiwan can be punished for transacting with individuals and entities included in any of OFAC lists. For this very reason, loads of registries and registrars decide to preemptively block all transactions with targets of sanctions even though not being officially bound to OFAC rulings. For instance, registrars Webglobe, EspaceCode, and Aerotek –respectively based in Slovakia, Canada, and Turkey– mention OFAC sanctions in their registrar-registrant agreements and explicitly state that they will not provide any services to those included in its lists.[28] Likewise, registries for the *.hn*, *.gg,* and *.je* ccTLDs –located in Honduras and in the Bailiwicks of Guernsey and Jersey– heedlessly follow OFAC rulings, telling registrars and other potential customers that they will not make any deals if an OFAC targeted individual or entity is made part of a contract.[29]

Here, the first explanation as to why this happens frames the phenomenon as strictly accidental, mentioning that it is all due to a foolish dynamic of «copy and paste» of the terms and conditions of service from one registry/registrar to the next what, unintendedly, makes non-U.S. based registries and registrars mention OFAC sanctions when they would not have to (CCWG-ACCT-WS2, 2018). But then, indeed, there is the option of explaining non-U.S. operators' behavior as mediated by the fear of being subject to «secondary» sanctions. As noted by the internet governance scholar Farzaneh Badiei, "it is simply too expensive to risk getting fined by OFAC" (Badiei, 2022a). If found to be transacting with an individual or entity included in its lists, non-U.S. registries and registrars could face punishments such as being excluded from U.S. markets, being barred from using the US$, or even facing criminal charges in the United States. Therefore, it is no wonder why many non-U.S. registries and registrars overcomply with OFAC[30].

As noticed by Clara Portela, overcompliance with OFAC programs by non-U.S.-based registries and registrars is hardly a trait singular to them since other non-U.S. entities operating in markets quite different from that of the DNS act in pretty much the same fashion. For instance, Portela shows that pursuant to the exacerbation of OFAC sanctions targeting Iran, in 2018, plenty of non-U.S. entities trading in areas as different as banking, industrial manufacturing, or health services decided on preemptively blocking all transactions involving Iranians (Portela, 2021; vid. Sahimi, 2022). And work by Ethan Kessler shows that this was the prevalent behavior of non-U.S. entities in all sorts of businesses involving Cuban counterparts (Kessler, 2022). Indeed, the fear of being subject to secondary sanctions permeates all areas included by OFAC in its sanction programs. Therefore, precautions taken by non-U.S. registries and registrars are not unique or peculiar to them but part of a more significant, intersectoral trend of preemptively blocking transactions that could make an entity subject to OFAC's secondary sanctions.

5. Escaping OFAC?

Arizona-based law professor Orde Kittrie wittingly pointed out in his latest take on the subject of «lawfare» that OFAC sanctions should be considered a form of "economic lawfare" (Kittrie, 2016:28). This peculiar term was first introduced by the retired general of the U.S. Air Force Charles J. Dunlap in a 2008 article as a means of naming "the strategy of using –or misusing– law as a substitute for traditional military means to achieve an operational objective" (Dunlap, 2008:146). Since then, the concept of lawfare has stretched out a bit, and Dunlap himself has helped further shape its meaning. By his latest definition, lawfare stands for "the use of law as a means of accomplishing what should otherwise require the application of force, or as a means of facilitating the same" (Dunlap, 2015:824).

Thus defined, it seems on point that Kittrie counts OFAC sanctions as a form of economic lawfare. First, as these sanctions are routinely put in place as a means of curtailing or crippling the operational capabilities of "America's enemies", avoiding the need to resort to brute force (vid. Zarate, 2013). And second, as OFAC rulings help the U.S. shape a global economic landscape favorable to its interests without employing "bloody, expensive, and destructive forms of warfare" (Kittrie, 2016:3). Following Dunlap's seminal work, lawfare is now a thoroughly examined and thriving line of research (vid. Werner, 2010). However, most analysts use it as a "pejorative concept" (Horton, 2010). For instance, Brooke Goldstein, head of *The Lawfare Project*, uses the concept to talk about "the abuse of the law and legal systems for strategic political or military ends" (Goldstein, 2010). And Jeff Handmaker uses it to frame "the illegitimate/hegemonic use of the law" by the state, calling lawfare a threatening form "of legal instrumentalism" (Handmaker, 2019).

Nevertheless, some frame lawfare in a much more benevolent light, theorizing that it "encourages using law instead of military force" to achieve operational objectives, thus "civilizing" inter-state conflict (vid. Scharf & Andersen, 2010:17 ss.). U.S. advocates of the *positive* reading of lawfare tend to resort to examples such as the one concerning Iran, or the more recent involving Russia, to back up their claims that economic lawfare actions –for instance, comprehensive sanctions programs, the statutory blockade of financial assets, etc.– have helped in avoiding direct military conflict with targets of those very actions (vid. Finkelstein et al., 2023; Bowman,

[28] The terms and conditions of service of the registrars Webglobe, EspaceCode and Aerotek can be found at https://perma.cc/EXZ3-BYKH, https://perma.cc/P8BV-BPVE and https://perma.cc/47K6-ZTRF.

[29] The terms and conditions of service of the registries in charge of the *.hn*, *.gg* and *.je* namespaces can be found at https://perma.cc/W563-E6BF and https://perma.cc/LXU8-54NX.

[30] This article uses the term overcompliance as defined by Law Professor Pierre-Hugues Verdier: "A situation in which a market participant applies sanctions that is, refrains from an otherwise desirable transaction or activity involving some connection with a sanctioned country or person beyond what is legally mandated by the relevant regime" (Verdier, 2023:474).

2021). And far away from the U.S., there is also a fair share of researchers and pundits advancing the idea that lawfare is the best tool to avoid direct military confrontation when inter-state problems arise (vid. Kittrie, 2016).

Regardless of the position one takes in the *positive vs. negative* lawfare toning debate, what seems relatively clear is that the way OFAC sanctions have been applied to the DNS makes for a steady case of this phenomenon. First, as the U.S. has routinely leveraged its jurisdictional powers over ICANN and both U.S.-based registries and registrars, turning them into tools aimed at battling «America's enemies» by juridical, statutory means. And second, as non-U.S.-based registries and registrars have been fearfully persuaded to comply with OFAC programs through «secondary sanctions», thus amplifying the extent and impact of its sanctioning efforts.

Indeed, as shown in Section 4, OFAC sanctions have been used by the U.S. administration to conduct –sometimes massive– domain name seizures and to persuade, so to prevent, (even) non-U.S. registries and registrars from transacting with individuals and entities targeted by OFAC sanctions. Conjointly, OFAC sanctions were –and still are– deployed to prevent ICANN from accrediting entities from sanctioned countries to start performing gTLD registry and registrar functions.

Positively, these first two phenomena –i.e., the one relating to domain seizures and the one relating to preventing registries and registrars from doing business with OFAC sanctions targets– have very little to do with ICANN since the U.S. administration conducts both these endeavors without needing to resort to the corporation. However, the third one is very much an undertaking for which ICANN is paramount, since the corporation is the sole party in charge of accrediting gTLD registries and registrars to start performing such functions in the DNS.

As already advanced at the beginning of Section 4, the CCWG-ACCT-WS2 «jurisdiction» subgroup noticed that OFAC sanctions were a problem for ICANN, and they concocted a list with recommendations aimed at lessening its burden. Specifically, the «jurisdiction» subgroup recommended ICANN: (1) "to take steps to pursue [and obtain] one or more [OFAC] general licenses"; (2) to modify its «Base Registry Agreement» and «Registrar Accreditation Agreement», stating that if OFAC general licenses are not provided, the corporation would "use [its] best efforts to secure [exclusive authorizations]" on behalf of prospective gTLD registries and registrars; and (3) to approach non-U.S. registries and registrars, in order to inform them that they are not required to comply with OFAC sanctions programs (CCWG-ACCT-WS2, 2018).

For now, ICANN has only implemented the «jurisdiction» subgroup recommendation regarding the modification of the registry and registrar agreements (ICANN, 2022c). Up until 2022, the corporation stated that it was "under no obligation to seek [exclusive authorizations]" (ICANN, 2018). Nevertheless, starting last year, the registry and registrar agreements now mention that "ICANN commits to seek such licenses" (ICANN, 2022a). However, the corporation also explains that even if ICANN puts its best efforts into it, "OFAC could [still] decide not to issue a requested license" (ibid., 2022a).

Certainly, it has been celebrated that ICANN is starting to implement the WS2 «jurisdiction» subgroup recommendations. But the situation is far from ideal since OFAC sanctions, today, still severely hamper ICANN's capacity to adequately perform its role in helping sustain "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet" (ICANN, 2022b). Indeed, terms like «openness», «reliability», and «global» refuse a clear-cut interpretation and are prone to disparate readings. But all those concerned with the impact of OFAC sanctions over ICANN and the DNS coincide in seeing that such punitive measures hardly help make the Internet more open, reliable, or global (vid. Badiei, 2017; 2022a; CCWG-ACCT-WS2, 2018; Singh, 2016).

The current situation gives room for thinking of some alternatives by which ICANN could come to avoid the dent of OFAC sanctions. Thus, before concluding, this article will explore some tentative ways by which ICANN could come to avoid its effects. These proposals, indeed, carry their own dangers. They all trade OFAC sanctions for something else, and they should not be seen or taken as definitive, gilt-edged solutions. Indeed, they are just a collection of fancy games that carry their own set of technical complexities, legal uncertainties, or geopolitical dilemmas. Nonetheless, they are worth mentioning.[31]

The first and second proposals recycle the most meaningful bids made during WSIS and the IANA Stewardship Transition. As seen in Section 2, these proposals aimed at either (1) moving ICANN's headquarters outside of the United States; or (2) subjecting the corporation to oversight by the United Nations, be it by transferring ICANN's competencies to the International Telecommunication Union (ITU), or by making the corporation directly accountable to the UN. Positively, moving ICANN's headquarters outside of the U.S. would make the corporation *immune* to OFAC primary sanctions, as it would no longer be part of U.S. jurisdiction. Likewise, putting the UN on top of ICANN –or transferring its competencies to ITU– would forcibly mean getting rid of OFAC's jurisdictional dominion, as sanctions would be applied only if approved by the United Nations Security Council (UNSC).[32]

Indeed, if applied, both these proposals would render the OFAC problem meaningless. Nevertheless, some other problems might emerge. If ICANN decided to change its place of incorporation, the government of that country could enforce sanctions over ICANN in pretty much the same way as the U.S. has done with OFAC. Therefore, the problem would remain the same only but in name. Even countries praised for their longstanding *neutrality* or international restraint, like Switzerland, Ireland, or Liechtenstein, hold their own sanctions programs, and could enforce them over ICANN if the corporation came to be inside their jurisdiction. Certainly, none of these countries has a sanctions apparatus as hefty –and overreaching– as that of the United States, and, on this wise, moving the

[31] As already mentioned in the introduction, this article focuses on analyzing some courses of action that could be taken by ICANN in order to avoid compliance with OFAC sanctions programs. Therefore, in what follows, this article does not include any details on proposals aimed at helping registrars, registries or other DNS operators (e.g. authoritative nameserver administrators, DNS hosting services, etc.) escape OFAC.

[32] The UN Security Council is entitled to take sanctioning measures under Article 41 of the United Nations Charter. Since 1966, its sanctioning efforts have taken quite a different number of forms: "The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions" (UNSC, 2022).

corporation's headquarters to any of them would surely make the sanctions problem less pervasive. But still, at some point, these countries could find it fitting to recklessly expand their sanctioning efforts, thus making the situation somewhat parallel to the one ICANN faces today.

The option of putting the UN on top of ICANN, or the one aiming at transferring its functions to ITU, certainly entail some dangers of their own. For starters, sanctions-wise, the UN system is quite flawed, as sanctions need to be cleared out by the UN Security Council (UNSC). Members of the UNSC with veto powers –China, France, Russia, the UK, and the United States– can block resolutions, for instance, regarding sanctions proposals (vid. De Wet, 2004). Positively, even in this politically charged environment, resolutions come to be passed on those rare occasions in which all members agree and, also, when one or several of the countries vested with veto powers are absent from voting sessions.[33] As noted by David L. Bosco, this procedure makes UN sanctions prone to instrumentalization in a game of power politics that, ultimately, makes them somewhat unstable (Bosco, 2009). Sanctions come and go as those involved in the security council, especially countries with veto powers, clinch on deals that come to their advantage. Therefore, if found to be included inside this *modus operandi*, sanctions affecting ICANN's capacity to accredit gTLD registrars and registries could turn all the more damaging, at the very least in terms of the impact they would have over the «reliability» of the Domain Name System. The DNS is functional insofar as users and content providers know what is and is not part of it. Therefore, making ICANN subject to a system in which sanctions pop up and then suddenly about-face –which is quite the common tendency in the UNSC ecosystem (vid. Vreeland & Dreher, 2014; Dörfler, 2019)– would make «reliability» a requisite quality absent of it all.

However, the most probable scenario is that neither the first nor the second proposals will ever be applied. In 2014, at the start of the IANA Transition, the U.S. administration made it very much clear that it would not (ever) accept changes in the way the DNS was administered that entailed substituting U.S. oversight of ICANN operations "with a government-led or an inter-governmental organization solution" (NTIA, 2014). And ever since then, ICANN has upheld this idea when confronted with the prospect of moving its headquarters outside of the U.S. or letting itself be commanded by the United Nations (NTIA, 2015; Rosenzweig, 2015).

Leaving the first and second proposals aside, a third option would entail unbinding ICANN from compliance with OFAC, and letting the corporation develop its own sanctions policy in tandem with other –community-led– Internet actors. This very idea has recently been furthered by a relatively broad compound of researchers, cybersecurity experts, content and service providers, and entities like the Internet Archive –and even by three MPs of the European Parliament– in a policy proposal named *Multistakeholder Imposition of Internet Sanctions* (MIIS, 2022).

As mentioned by Niels Ten Oever (one of the signatories of the MIIS proposal), the whole idea would be to let internet governance actors get "the means to develop sanctions in a coordinated, open, and voluntary manner" (Ten Oever, 2022). Specifically, as developed in the MIIS proposal, this would mean forming "a new, minimal, multistakeholder mechanism, similar in scale to NSP-Sec or Outages,[34] which after due process and consensus would publish sanctioned IP addresses and domain names in the form of public data feeds in standard forms" (MIIS, 2022). Lists compiled with this new «mechanism» would be developed "us[ing] clearly documented procedures to assess violations of international norms in an open, multistakeholder, and consensus-driven process, taking into account the principles of non-overreach and effectiveness in making its determinations" (ibid, 2022).

Certainly, if applied, the MIIS program would entail a radical change in the way sanctions are designed and enforced. For starters, sanctions proposals would be devised and put forth by a community of individuals based in different parts of the world. And this much, indeed, would mean that such sanctions are not put in place just to help a country in bringing about a bevy of its self-centered economic, political, or national security objectives. Surely, the MIIS system could turn into a hogwash discussion group without a meaningful capacity to reach a consensus regarding the sanctions to be imposed upon individuals or entities. And, indeed, there is the risk that the "open, multistakeholder, and consensus-driven process" that the MIIS advocates could turn into a one-sided effort held and sustained by a cluster of frequent and active stakeholders (vid. Badiei, 2022b). In its current state, the proposal is vague and perilous since it would be easy for interested parties to tilt it and make the system unbalanced. Therefore, much work is needed to turn the MIIS proposal into something that could be implemented without risking collapse.

A fourth –and for the purposes of this article, final– option aimed at dispatching ICANN from compliance with OFAC sanctions would require the U.S. administration giving the corporation "partial immunity" from U.S. laws. This idea was advanced by Brazilian representatives participating in the WS2 «jurisdiction» subgroup discussions, and it has been recently picked up by some stakeholders finding ICANN's post-IANA Transition reforms insufficient. As presented during the WS2 discussions, the proposal consisted in asking the U.S. government on giving ICANN a special status, like the one currently enjoyed by the International Fertilizer and Development Center (IFDC), headquartered in Alabama, "whose immunity from U.S. jurisdiction [was] obtained through a Presidential Decree in

[33] In the UNSC, it's been quite common for states to push sanctions resolutions when states with veto powers positioned against such measures are absent of voting sessions. Here, the most famous example is that of the U.S. pushing sanctions in 1950 against North Korea in a voting session the USSR was absent from.

[34] NSP-Sec is a volunteer incident response mailing list, concerned with tracking exploits and compromised ISPs and NSPs systems. The group tries to mitigate attacks on those very systems by circulating a list with the exploits found by its members. In turn, Outages is a wiki and mailing list concerned with providing a comprehensive list of planned and unplanned network outages and for reporting failures in major communications infrastructure components having significant traffic-carrying capacity. Information about NSP-Sec and Outages can be found at https://puck.nether.net/mailman/listinfo/nsp-security and https://puck.nether.net/mailman/listinfo/outages.

1977, under the U.S. International Organizations Immunities Act (IOIA)" (CCWG-ACCT-WS2, 2018: Annex 4.2). Other organizations currently enjoying "partial immunity" under IOIA include the Inter-American Statistical Institute (IASI), the International Monetary Fund (IMF), the Organization for Economic Cooperation and Development (OECD), and the World Health Organization (WHO).[35]

As it was advanced by the Brazilian representatives participating in WS2, this proposal would consist in giving ICANN «immunity» just concerning OFAC sanctions programs while keeping the corporation subject to the rest of U.S. federal and California laws (ibid., 2018: Annex 4.2). Nevertheless, the United States Code (USC) and IOIA include some requirements for obtaining "partial immunity" that ICANN might not fulfill. As defined in §288, Title 22 (Subchapter XVIII) of the USC, the United States administration only takes into consideration immunity requests made by –or targeting– "public international organization[s] in which the United States [government] participates pursuant to any treaty or under the authority of any Act of Congress authorizing such participation or making an appropriation for such participation" (USC, 2023).

Certainly, ICANN is not a public international organization, but a "nonprofit public benefit corporation" (vid. ICANN, 2016b). And, what's more, since completing the IANA Transition, in 2016, the United States administration no longer participates in any capacity in ICANN. At present, these two barriers might make it nearly impossible for ICANN to be given "partial immunity" under IOIA. However, IOIA and the USC include some examples of organizations that have been given immunity even when not being «public international organizations» participated by the U.S. administration.[36] Here, the most notable (or high-profile) case is, indeed, that of the International Committee of the Red Cross (ICRC). The ICRC is "an atypical international organization" since it is "more similar to a private or non-governmental organization (NGO)" than to the standard public international organization (IO) directly governed or participated by States (Debuf, 2016: 321–323). The ICRC is governed by a body of private individuals, and no nation-state holds any position or capacity inside the organization. Nevertheless, the ICRC "has come to be granted a legal status and treatment equivalent to that of an IO […] enjoy[ing] both international legal personality and privileges and immunities in both the international and domestic legal orders" (ibid. 2016:324).

Taking the ICRC as an example, ICANN could try to persuade the U.S. administration on extending it the same treatment and giving it "partial immunity", though the U.S. government could certainly refuse to do so on grounds that the corporation does not qualify –by law, as specified in IOIA and the USC– for such special treatment. Positively, giving ICANN "partial immunity" would make the OFAC problem disappear. But, here again, some unintended problems might emerge if this design is not properly executed. As commented by some stakeholders during the WS2 discussions, giving ICANN immunity "could also mean [giving it] immunity […] from the kind of accountability to basic forms of law that the [ICANN community] wants ICANN to have" (Digital Watch Observatory, 2017). Ergo, extreme caution would be required if asking the U.S. administration for such special treatment, since awarding the corporation "partial immunity" might give way to a situation where ICANN could potentially misuse its powers without adequate recourse or consequences.

6. Conclusions

The IANA Stewardship Transition, completed on October 1, 2016, marked an important milestone in ICANN's journey towards independence from U.S. direct oversight. Indeed, the transition transferred complete control of the IANA functions to the corporation, finally ending eighteen years of supervision by the U.S. National Telecommunications Administration (NTIA). However, ICANN remains subject to U.S. jurisdiction, and with it, to the Office of Foreign Assets Control (OFAC) economic and trade sanctions programs.

After completing the IANA Transition, the CCWG-ACCT-WS2 «jurisdiction» subgroup gave ICANN some recommendations aimed at helping the corporation mitigate the impact of OFAC sanctions. But while recommendations put forth by the «jurisdiction» subgroup are much laudable, they do not seem to be able to solve most of the problems OFAC sanctions pose for ICANN. Undoubtedly, it is praiseworthy that ICANN took heed of WS2 recommendations, implementing changes to its «Base Registry Agreement» and its «Registrar Accreditation Agreement» aimed at helping prospective registries and registrars escape OFAC sanctions. Nevertheless, if ICANN wants to escape OFAC's grasp effectively –and thoroughly– much work is yet to be done.

To this aim, several options –listed in Sec. 5 of this article– remain within ICANN's reach. Nevertheless, all these options carry their own technical complexities, legal uncertainties, or geopolitical dilemmas. Indeed, the main takeaway this article has to offer is that there are no gilt-edged solutions to the OFAC quandary. ICANN has gone to great lengths to make itself better suited to perform its given role as the administrator of some crucial aspects of the DNS. And it is much needed that the corporation keeps doing so. However, to do that, ICANN would need to listen not only to its «Empowered Community» but to the Internet community as a whole. CCWG-ACCT-WS2 recommendations offer some guidance, but a broader and more comprehensive strategy is needed to navigate the complex landscape of U.S. sanctions, thus ensuring ICANN's ability to fulfill its responsibilities effectively.

Ultimately, this article has tried to contribute to the ongoing debate about sanctions affecting Internet systems and services. On this front, some promising work has been developed as of late by Farzaneh Badiei, Angie Orejuela, and Ryan Pan at Digital Medusa, by Natalie Campbell and Carl Gahnberg at ISOC, or by Tamlin Magee and Ewa Dąbrowska at different media and research outlets (Badiei

[35] The list of organizations enjoying partial immunity under the International Organizations Immunities Act (IOIA) is periodically updated in Title 22, Subchapter XVIII, of the United States Code (USC). The most recent version of the USC can be accessed at https://uscode.house.gov/download/download.shtml.

[36] Organizations that have been given partial immunity under IOIA even if not being public international organizations participated by the U.S. government include –among others– the Organization of Eastern Caribbean States (OECS), the European Space Agency (ESA), the International Committee of the Red Cross (ICRC), the African Union (AU), and the Global Fund to Fight AIDS, Tuberculosis and Malaria (GFATM).

et al., 2023; Campbell & Gahnberg, 2022; Dąbrowska, 2022; Magee, 2022). Nevertheless, further research is needed in order to properly assess the extent, significance, and distinct geographical impact of sanctions affecting Internet systems and services. Moreover, specifically regarding the DNS, additional research is needed not only providing a deeper assessment of the impact and effects of sanctions programs on ICANN and on domain names registries and registrars, but also on other DNS operators such as authoritative nameserver administrators or DNS hosting services.

Carrying-out additional research on topics as the ones outlined above is essential to gain a deeper understanding of whether OFAC sanctions have distinct effects on Internet systems and services as compared to other areas. This article has tried to shed some light on the effects of OFAC sanctions on ICANN, while also providing some preliminary notes on the effects of such sanctions on domain name registries and registrars. Nevertheless, there remains a need to explore the implications for other critical actors both within the DNS and the broader Internet ecosystem.

It seems equally important to extend research efforts to analyze other sanctioning regimes, carried out by actors other than OFAC. Sanctions imposed by other branches of the U.S. government –most notably, by the Bureau of Industry and Security (BIS)– but also by other countries and by supranational organizations like the European Union (EU), present their own unique challenges and implications for Internet systems and services. Therefore, research should be extended to encompass these other actors, with the aim of developing a more comprehensive and detailed account on how sanctions jointly affect the myriad of digital technologies, services and entities that make up the Internet and support its various functions.

Declarations of competing interest

None.

References

Badiei, F. (2017). "ICANN's jurisdiction: Sanctions and domain names". *Internet Governance Project*.

Badiei, F. (2022a). ONEWORLD.SOMEINTERNET: New gTLD registries and sanctioned countries". *CircleID*. https://circleid.com/posts/20220217-oneworld-.someinternet-new-gtld-registries-and-sanctioned-countries. (Accessed 30 June 2023).

Badiei, F. (2022b). How to multistakeholder wash Internet disconnection: On the multistakeholder Internet governance sanction regime. *Digital Medusa*. https://digitalmedusa.org/how-to-multistakeholder-wash-internet-disconnection-on-the-multistakeholder-internet-governance-sanction-regime/. (Accessed 30 June 2023).

Badiei, F., Orejuela, A., & Pan, R. (2023). *Sanctions and the Internet*. Digital Medusa/RIPE NCC. https://digitalmedusa.org/wp-content/uploads/2023/05/SanctionsandtheInternet-DigitalMedusa.pdf. (Accessed 30 June 2023).

Benkler, Y. (2006). The Wealth of Networks. How social production transforms markets and freedom. In *New haven*. London: Yale University Press.

Bosco, D. (2009). *Five to rule them all. The UN security council and the making of the modern world*. Oxford: Oxford University Press.

Bowman, G. (2021). "Securing the precipitous heights: U.S. Lawfare as a means to confront China at sea, in space, and cyberspace". *Pace International Law Review, 34/1*, 81–123.

Boyle, A. (2021). "Checking the president's sanctions powers. A proposal to reform the international emergency economic powers act". *Brennan Center for Justice at New York University School of Law*. June 2021.

Bradshaw, S., & DeNardis, L. (2016). "The politization of the Internet's domain name system: Implications for internet security, universality, and freedom". *New Media & Society, 20/1*, 1–19.

Brühl, T., & Rittberger, V. (2001). "From international to global governance: Actors, collective decision-making, and the United Nations in the world of the twenty-first century". In V. Rittberger (Ed.), *Global governance and the united nations system*. New York: United Nations University Press.

Campbell, N., & Gahnberg, C. (2022). How refusing Russian networks will impact the internet. *Internet Society*. https://www.internetsociety.org/wp-content/uploads/2022/03/IIB-Russian-Network-Refusals.pdf. (Accessed 30 June 2023).

Carr, M. (2016). *U.S. Power and the internet in international relations. The irony of the information age*. London: Palgrave Macmillan.

Casey, R. (2008). *ICANN or ICANN't represent internet users*. Blacksburg: Virginia Polytechnic Institute and State University.

Cavalli, O., & Scholte, J. (2021). The role of states in internet governance at ICANN. In B. Haggart, N. Tusikov, & J. Scholte (Eds.), *Power and authority in internet governance. Return of the state?* London: Routledge.

CCWG-ACCT-WS2. (2018). Final report. *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/system/files/files/ccwg-acct-ws2-final-24jun18-en.pdf. (Accessed 30 June 2023).

CDT. (2016). "Civil society statement of support for IANA transition". *Center for Democracy & Technology*. https://cdt.org/insights/civil-society-statement-of-support-for-iana-transition/. (Accessed 30 June 2023).

CEI. (2016). CEI joins coalition urging congress to pause the IANA transition. *Competitive Enterprise Institute*. https://cei.org/coalition_letters/cei-joins-coalition-urging-congress-to-pause-the-iana-transition/. (Accessed 30 June 2023).

CHE Project. (2013). "OFAC licensing". *Counterterrorism and Humanitarian Engagement Project, Harvard Law School*. https://blogs.harvard.edu/cheproject/files/2012/10/CHE-Project-OFAC-Licensing.pdf. (Accessed 30 June 2023).

Clausing, J. (1999). *Network solutions reports record earnings*. The New York Times. https://archive.nytimes.com/www.nytimes.com/library/tech/99/04/cyber/articles/22nsi.html. (Accessed 30 June 2023).

Cloudflare. (2022). *United States securities and exchange commission: Form 10-Q*. Cloudflare Inc. https://cloudflare.net/files/doc_financials/2022/q1/5136f41b-4473-4704-a1d1-029aa4810a4e.pdf. (Accessed 30 June 2023).

Cloudflare. (2023). What are the different types of DNS server? *Cloudflare DNS Glossary*. https://www.cloudflare.com/learning/dns/dns-server-types/. (Accessed 30 June 2023).

Cogburn, D. (2017). *Transnational advocacy networks in the information society. Partners or pawns?* London: Palgrave Macmillan.

Cogburn, D., Mueller, M., McKnight, L., Klein, H., & Mathiason, J. (2005). The U.S. Role in global internet governance. *IEEE Communications Magazine*. December 2005.

Committee to Protect Journalists. (2021). "CPJ calls on U.S. to publish list of all websites recently seized in sanctions crackdown". *Counselling and Psychotherapy Journal*. https://cpj.org/2021/06/cpj-calls-on-u-s-to-publish-list-of-all-websites-recently-seized-in-sanctions-crackdown/. (Accessed 30 June 2023).

Corwin, P. (2016). "The irritating irresolution of ICANN jurisdiction". CircleID. https://circleid.com/pdf/ICANN_Jurisdiction_FINAL_Long.pdf. (Accessed 30 June 2023).

Dąbrowska, E. (2022). Digital sanctions against Russia and geopolitization of the Internet. *SCRIPTS*. https://www.scripts-berlin.eu/publications/blog/Blog-63-Dabrowska-Internet-Gov/index.html. (Accessed 30 June 2023).

Davis, S., & Ness, I. (2022). *Sanctions as war. Anti-imperialist perspectives on American geo-economic strategy*. Leiden: Brill.

De Vey, K., & Rijgersberg, R. (2006). "Rethinking accountability in cyberspace, A new perspective on ICANN". *International Review of Law, Computers & Technology, 21/1*, 1–11.

De Vey, K., & Rijgersberg, R. (2015). "Internet Governance and Global Self Regulation. Theoretical and empirical building blocks for a general theory of self regulation". *Legisprudence, 4/3*, 385–404.

De Wet, E. (2004). *The chapter VII powers of the united nations security council*. Portland: Hart Publishing.

Debuf, E. (2016). "Tools to do the job: The ICRC's legal status, privileges and immunities. *International Review of the Red Cross, 97*, 319–344.

Digital Watch Observatory. (2017). "Jurisdiction issues in focus at ICANN60". *Digital Watch Observatory – Geneva Internet Platform*. https://dig.watch/event/icann60-abu-dhabi/jurisdiction-icann60. (Accessed 30 June 2023).

Dörfler, T. (2019). *Security council sanctions governance. The power and limits of rules*. London: Routledge.

Drake, W. (2016). "Why the WGIG still matters". In W. J. Drake (Ed.), *The working group on internet governance. 10th anniversary reflections*. Johannesburg: The Association for Progressive Communications.

Drazek, K., Carter, J., Kleinwachter, W., Mueller, M., Rickert, T., Tropina, T., & Tonkin, B. (2022). *ICANN's Accountability and Transparency: A Retrospective on the IANA Transition*. https://www.internetgovernance.org/2022/09/17/icanns-accountability-and-transparency-a-retrospective-on-the-iana-transition/. (Accessed 30 June 2023).

Dunlap, C. (2008). "Lawfare today: A perspective". *Yale Journal of International Affairs, Winter, 2008*, 146–154.

Dunlap, C. (2015). "Lawfare". In J. Norton, G. Roberts, & R. Turner (Eds.), *National security law & policy*. Durham: Carolina Academic Press.

Finkelstein, C., Fuller, C., Ohlin, J., & Regan, M. (2023). *Between crime and war: Hybrid legal frameworks for asymmetric conflict*. Oxford: Oxford University Press.

Froomkin, M., & Lemley, M. (2003). "ICANN and antitrust". *University of Illinois Law Review, 1*, 1–76.

Geranmayeh, E., & Lafont, M. (2019). "Meeting the challenge of secondary sanctions". *European Council on Foreign Relations*. https://ecfr.eu/publication/meeting_the_challenge_of_secondary_sanctions/. (Accessed 30 June 2023).

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. New York: Oxford University Press.

Goldstein, B. (2010). "Lawfare: Real threat or illusion?". *The Lawfare Project*. https://www.thelawfareproject.org/analysis/2010/11/5/ilawfare-real-threat-or-illusionibrthe-lawfare-project. (Accessed 30 June 2023).

Handmaker, J. (2019). "Researching legal mobilisation and lawfare". *International Institute of Social Studies*. Working Paper No. 641.

Held, D., & McGrew, A. (2000). "The great globalization debate: An introduction". In D. Held, & A. McGrew (Eds.), *The global transformations reader. Cambridge/*. Malden: Polity Press.

Horton, S. (2010). "The dangers of lawfare". *Case Western Reserve Journal of International Law, 43/1*, 163–179.

IANA-STCG. (2016). "Proposal to transition the stewardship of the internet assigned numbers authority (IANA) functions from the U.S. Commerce department's national Telecommunications and information administration (NTIA) to the global multistakeholder community". *IANA Stewardship Transition Coordination Group*. https://www.ianacg.org/icg-files/documents/IANA-transition-proposal-final.pdf. (Accessed 30 June 2023).

ICANN. (2000). "Memorandum of understanding between the U.S. Department of Commerce and internet corporation for assigned names and numbers". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en. (Accessed 30 June 2023).

ICANN. (2006). Annual report 2005–2006. *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/system/files/files/annual-report-2005-2006-en.pdf. (Accessed 30 June 2023). ".

ICANN. (2009). "ICANN strategic plan, july 2009 – June 2012". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/system/files/files/strategic-plan-2009-2012-09feb09-en.pdf. (Accessed 30 June 2023).

ICANN. (2012a). "Registrar accreditation: Financial considerations". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/pages/financials-55-2012-02-25-en. (Accessed 30 June 2023).

ICANN. (2012b). "gTLD applicant guidebook". *Internet Corporation for Assigned Names and Numbers*. https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf. (Accessed 30 June 2023).

ICANN. (2012c). "ICANN strategic plan, july 2012 – June 2015". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/system/files/files/strategic-plan-2012-2015-18may12-en.pdf. (Accessed 30 June 2023).

ICANN. (2013a). "Montevideo statement on the future of internet cooperation". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/announcements/details/montevideo-statement-on-the-future-of-internet-cooperation-7-10-2013-en. (Accessed 30 June 2023).

ICANN. (2013b). "About resellers". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/pages/reseller-2013-05-03-en. (Accessed 30 June 2023).

ICANN. (2014). "Endorsements of the IANA globalization process". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/system/files/files/globalization-endorsements-18mar14-en.pdf. (Accessed 30 June 2023).

ICANN. (2016a). "Stewardship of IANA functions transitions to global internet community as contract with U.S. Government ends". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en. (Accessed 30 June 2023).

ICANN. (2016b). "Amended and restated articles of incorporation of internet corporation for assigned names and numbers". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/pages/governance/articles-en. (Accessed 30 June 2023).

ICANN. (2017). "Base registry agreement". *Internet Corporation for Assigned Names and Numbers*. https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf. (Accessed 30 June 2023).

ICANN. (2018). "ICANN registrar accreditation application form – 19 september 2018 archived application". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/system/files/files/raa-application-form-17sep18-en.docx. (Accessed 30 June 2023).

ICANN. (2022a). "ICANN registrar accreditation application form". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/resources/registrars/accreditation/application-form.docx. (Accessed 30 June 2023).

ICANN. (2022b). "Bylaws for internet corporation for assigned names and numbers". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/pages/governance/bylaws-en/. (Accessed 30 June 2023).

ICANN. (2022c). "Update on ICANN work Stream 2 implementation". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/en/blogs/details/update-on-icann-work-stream-2-implementation-02-05-2022-en. (Accessed 30 June 2023).

ICANN. (2023). "ICANN documentary information disclosure policy". *Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/pages/didp-2023-01-24-en. (Accessed 30 June 2023).

ISOC. (2016). "IANA transition". *Internet Society*. https://www.internetsociety.org/iana-transition/. (Accessed 30 June 2023).

Jeftovic, M. (2018). *Managing mission-critical domains and DNS*. Sebastopol: O'Reilly.

Kacowicz, A. (2012). Global governance, international order, and world order. In D. Levi-Faur (Ed.), *The oxford handbook of governance*. Oxford: Oxford University Press.

Kesan, J., & Gallo, A. (2008). "Pondering the politics of private procedures: The case of ICANN". *I/S: A Journal of Law and Policy for the Information Society, 4*, 345–409.

Kessler, E. (2022). Working paper: How economic sanctions are used in U.S. Foreign policy. *The Chicago Council on Global Affairs*. March 2022.

Kittrie, O. (2016). *Lawfare. Law as a weapon of war*. New York: Oxford University Press.

Kleinwächter, W. (2009). "Good governance of the borderless internet: Who should do what?". *Telos, 80*, 1–20.

Kleinwächter, W. (2016). Breaking nonsense: Ted Cruz, IANA transition and the irony of life. CircleID. https://circleid.com/posts/20160921_breaking_nonsense_ted_cruz_iana_transition_and_irony_of_life. (Accessed 30 June 2023).

Kovacs, A., Githaiga, G., & Varon, J. (2014). "Netmundial: Reflections from Brazil, India and Kenya". *Global Partners Digital, Paper No. 2*. September 2014.

Krebs, B. (2013). "Trade sanctions cited in hundreds of Syrian domain seizures". *Krebs on Security*. https://krebsonsecurity.com/2013/05/trade-sanctions-cited-in-hundreds-of-syrian-domain-seizures/. (Accessed 30 June 2023).

Lipscy, P. (2017). *Renegotiating the world order. Institutional change in international relations*. Cambridge: Cambridge University Press.

Liptak, A. (2008). “A wave of the Watch list, and speech disappears”. *The New York Times*. https://www.nytimes.com/2008/03/04/us/04bar.html?_r=1. (Accessed 30 June 2023).

Lohmann, S. (2019). “Extraterritorial U.S. Sanctions”. *German Institute for International and Security Affairs, SWP Comments, 5*.

Magee, T. (2022). “Why digital sanctions are the latest geopolitical battleground”. *Raconteur*. https://www.raconteur.net/growth-strategies/digital-sanctions-latest-battleground/. (Accessed 30 June 2023).

Malcolm, J. (2008). *Multi-stakeholder governance and the internet governance forum*. Perth: Terminus Press.

Meyer, J. (2009). “Second thoughts on secondary sanctions”. *University of Pennsylvania Journal of International Law*, 905–968.

MIIS. (2022). “Multistakeholder imposition of internet sanctions”. *Computable nl*. https://www2.computable.nl/uploads/pdf/multistakeholder-imposition-of-internet-sanctions.pdf. (Accessed 30 June 2023).

Mockapetris, P. (1983a). “Domain names – concepts and facilities”. *(RFC 882). Internet Engineering Task Force*.

Mockapetris, P. (1983b). “Domain names – implementation and specification”. *(RFC 883). Internet Engineering Task Force*.

Mueller, M. (2002). Ruling the root. Internet governance and the taming of cyberspace. In *Cambridge*. London: The MIT Press.

Mueller, M. (2010). Networks and states. The global politics of internet governance. In *Cambridge/*. London: The MIT Press.

Mueller, M. (2014). “Detaching internet governance from the state: Globalizing the IANA”. *Georgetown Journal of International Affairs – International Engagement on Cyber IV*, 35–44.

Mueller, M. (2015). “The IANA transition and the role of governments in internet governance”. *IP Justice Journal*.

Mueller, M., & Badiei, F. (2017). “Governing internet territory: ICANN, sovereignty claims, property rights and country code top-level domains”. *The Columbia Science & Technology Law Review, 18*, 435–491.

Negro, G. (2019). “A history of Chinese global Internet governance and its relations with ITU and ICANN”. *Chinese Journal of Communication, 13/1*, 104–121.

Neylon, M. (2016). “Heritage holding anti-IANA transition event with Cruz”. CircleID. https://circleid.com/posts/9803/11308/. (Accessed 30 June 2023).

NSF. (1995). “The internet grows up”. *National Science Foundation*. https://www.nsf.gov/news/news_summ.jsp?cntn_id=100806. (Accessed 30 June 2023).

NTIA. (2000). “IANA functions contract”. *National Telecommunications and Information Administration*. https://ntia.gov/files/ntia/publications/ianacontract.pdf. (Accessed 30 June 2023).

NTIA. (2005). “U.S. Principles on the Internet’s domain name and addressing system”. *National Telecommunications and Information Administration*. https://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system. (Accessed 30 June 2023).

NTIA. (2014). “NTIA announces intent to transition key internet domain name functions”. *National Telecommunications and Information Administration*. https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions. (Accessed 30 June 2023).

NTIA. (2015). “Testimony of assistant secretary strickling on internet governance progress after ICANN 53”. *National Telecommunications and Information Administration*. https://www.ntia.doc.gov/speechtestimony/2015/testimony-strickling-internet-governance-progress-after-icann-53. (Accessed 30 June 2023).

OFAC. (2002). “What is OFAC and what does it do?”. *U.S. Department of the Treasury*. https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1. (Accessed 30 June 2023).

OFAC. (2006). “How long has OFAC been around?”. *U.S. Department of the Treasury*. https://home.treasury.gov/policy-issues/financial-sanctions/faqs/2. (Accessed 30 June 2023).

OFAC. (2015). “Who must comply with OFAC regulations?”. *U.S. Department of the Treasury*. https://home.treasury.gov/policy-issues/financial-sanctions/faqs/11. (Accessed 30 June 2023).

OFAC. (2019). “Executive order of august 5, 2019. Blocking property of the government of Venezuela. General license No. 25”. *U.S. Department of the Treasury*. https://ofac.treasury.gov/media/31761/download?inline. (Accessed 30 June 2023).

OFAC. (2022a). “Specially designated nationals and blocked persons list (SDN) human readable lists”. *U.S. Department of the Treasury*. https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists. (Accessed 30 June 2023).

OFAC. (2022b). “Russian harmful foreign activities sanctions regulations 31 CFR part 587. General license No. 25”. *U.S. Department of the Treasury*. https://ofac.treasury.gov/media/924326/download?inline. (Accessed 30 June 2023).

OFAC. (2023). “Selected general licenses issued by OFAC”. *U.S. Department of the Treasury*. https://ofac.treasury.gov/selected-general-licenses-issued-ofac. (Accessed 30 June 2023).

Palladino, N., & Santaniello, M. (2021). *Legitimacy, power, and inequalities in the multistakeholder internet governance. Analyzing IANA transition*. Cham: Palgrave Macmillan.

Portela, C. (2021). “Creativity Wanted. Countering the extraterritorial effects of U.S. sanctions”. *European Union Institute for Security Studies*. October 2021.

Prakash, P. (2016). Jurisdiction: The taboo topic at ICANN. *The Centre for Internet & Society*.

Rathbone, M., & Egan, B. (2017). “Coping with the US secondary sanctions tsunami”. *World: The Journal of Exports Controls and Sanctions*. https://www.steptoe.com/a/web/138504/SecondarySanctionsTsunami-WorldECR.pdf. (Accessed 30 June 2023).

Raustiala, K. (2016). “Governing the internet”. *American Journal of International Law, 110/3*, 491–503.

Raymond, M., & DeNardis, L. (2015). “Multistakeholderism: Anatomy of an inchoate global institution”. *International Theory, 7/3*, 572–616.

Rosenau, J., & Czempiel, E.-O. (1992). *Governance without government. Order and change in world politics*. New York: Cambridge University Press.

Rosenzweig, P. (2015). “On the issue of «jurisdiction» over ICANN”. *Lawfare*. https://www.lawfareblog.com/issue-jurisdiction-over-icann. (Accessed 30 June 2023).

RSSAC. (2016). “RSSAC023: History of the root server system”. *Root Server System Advisory Committee*. https://www.icann.org/en/system/files/files/rssac-023-04nov16-en.pdf. (Accessed 30 June 2023).

Rutkowski, A. (2018). “The meeting that changed the DARPA datagram internet”. CircleID. https://circleid.com/posts/20180113_the_meeting_that_changed_the_darpa_datagram_internet. (Accessed 30 June 2023).

Sahimi, M. (2022). A century of economic blackmail, sanctions and war against Iran. In S. Davis, & I. Ness (Eds.), *Sanctions as war. Anti-imperialist perspectives on American geo-economic strategy*. Leiden: Brill.

Sassen, S. (2007). *A sociology of globalization*. New York: W.W. Norton & Company.

Scharf, M., & Andersen, E. (2010a). Is lawfare worth defining – report of the cleveland experts meeting – september 11, 2010. *Case Western Reserve Journal of International Law, 43/1*, 11–27.

Singh, P. (2016). “Internet governance: Is the internet really free of U.S. Control?”. *Economic and Political Weekly, 51/43*, 27–30.

Stadnik, I. (2021). Russia. An independent and sovereign internet? In B. Haggart, N. Tusikov, & J. Scholte (Eds.), *Power and authority in internet governance. Return of the state?* London: Routledge.

Sun, M. (2019). “Cloud-Services company Cloudflare discloses potential sanctions violations”. *The Wall Street Journal*. https://www.wsj.com/amp/articles/cloud-services-company-cloudflare-discloses-potential-sanctions-violations-11568152033. (Accessed 30 June 2023).

Ten Oever, N. (2022). “Towards the multistakeholder imposition of internet sactions”. *Tech Policy Press*. https://techpolicy.press/towards-the-multistakeholder-imposition-of-internet-sanctions/. (Accessed 30 June 2023).

Trinkunas, H., & Wallace, I. (2015). “Converging on the future of global internet governance. The United States and Brazil”. *Brookings Institute*. July 2015.

UNCGG. (1995). United nations commission on global governance. *Global Governance Our Global Neighborhood*. https://archive.org/details/cmmn-on-global-governance-our-global-neighborhood-1995/mode/1up. (Accessed 30 June 2023).

UNSC. (2022). “Sanctions”. United nations security council. https://www.un.org/securitycouncil/sanctions/information. (Accessed 30 June 2023).

USC. (2023). United States code, 06/30/2023 release point. *Office of the Law Revision Counsel*. https://uscode.house.gov/download/download.shtml. (Accessed 30 June 2023).

U.S. Congress. (2006). "Internet governance: The future of ICANN. *Hearing before the Subcommittee on Trade, Tourism, and Economic Development of the Committee on Commerce, Science, and Transportations"*. *United States Congress*. https://www.govinfo.gov/content/pkg/CHRG-109shrg71638/html/CHRG-109shrg71638.htm. (Accessed 30 June 2023).

U.S. Congress. (2014). H.R. 5737. To prohibit the National Telecommunications and Information Administration from relinquishing responsibilities with respect to Internet domain name functions unless it certifies that it has received a proposal for such relinquishment that meets certain criteria, and for other purposes. *United States Congress*.

U.S. Congress. (2015). H.R. 2251. To prohibit the National Telecommunications and Information Administration from relinquishing responsibilities with respect to Internet domain name functions unless it certifies that it has received a proposal for such relinquishment that meets certain criteria, and for other purposes. *United States Congress*.

U.S. Congress. (2016a). H.R. 5418. To prohibit the national Telecommunications and information administration from allowing the internet assigned numbers authority functions contract to lapse unless specifically authorized to do so by an act of congress. *United States Congress*.

U.S. Congress. (2016b). S. 3034. To prohibit the national Telecommunications and information administration from allowing the internet assigned numbers authority functions contract to lapse unless specifically authorized to do so by an act of congress. *United States Congress*.

U.S. Department of Justice. (2020). United States seizes domain names used by Iran's islamic revolutionary guard Corps. *United States Department of Justice*. https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps. (Accessed 30 June 2023).

U.S. Department of Justice. (2021). "United States seizes websites used by the Iranian islamic radio and television union and kata'ib hizballah". *United States Department of Justice*. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib. (Accessed 30 June 2023).

Verdier, P.-H. (2023). "Sanctions overcompliance: What, why, and does it matter?". *North Carolina Journal of International Law, 48*, 471–498.

Vreeland, J., & Dreher, A. (2014). *The political economy of the United Nations security council. money and influence*. New York: Cambridge University Press.

Werner, W. (2010). "The curious career of lawfare". *Case Western Reserve Journal of International Law, 43/1*, 61–72.

WGIG. (2005). "Report of the working group on internet governance". *Working Group on Internet Governance*. https://www.wgig.org/docs/WGIGREPORT.pdf. (Accessed 30 June 2023).

Zarate, J. (2013). *Treasury's war. The unleashing of a new era of financial warfare*. New York: PublicAffairs.