The Politicization of the Internet's Domain Name System

Implications for Internet Security, Universality, and Freedom

Abstract: One of the most contentious and longstanding debates in Internet governance involves the question of oversight of the Domain Name System (DNS). DNS administration is sometimes understatedly described as a 'clerical' or 'merely technical' task, but it also implicates a number of public-policy concerns such as trademark disputes, infrastructure stability and security, resource allocation, and freedom of speech. A parallel but distinct phenomenon involves governmental and private forces increasingly altering or co-opting the DNS for political and economic purposes completely distinct from its core function of resolving Internet names into numbers. This paper examines both the intrinsic politics of the DNS in its day-to-day operations and specific examples and techniques of co-opting or altering DNS technical infrastructure as a new tool of global power. The article concludes with an analysis of the implications of this infrastructure-mediated governance on network security characteristics, architectural stability, and efficacy of the Internet governance ecosystem

Introduction

One of the most contentious debates in Internet governance involves the question of oversight of the Domain Name System (DNS). The DNS performs a straightforward function of resolving Internet domain names into numerical identifiers, thus many describe aspects of its oversight as a 'clerical' or 'merely technical' task. But the DNS also performs policymaking. Its design and administration implicates a number of public interest concerns such as trademark disputes, infrastructure stability and security, resource allocation, and free speech. There is also longstanding discord over the historic involvement of the US Department of Commerce (DOC) in overseeing aspects of DNS administration.

While these are contentious policy issues with implications for commerce, human rights, and Internet stability, it misses a parallel and distinct phenomenon in which governmental and private forces increasingly turn to the DNS for political and economic purposes completely distinct from its core functions. This phenomenon can be referred to as the "turn to infrastructure" in Internet governance (Author, 2012).

This paper fills a gap in policy and scholarship by examining both the intrinsic politics of the day-to-day operations within the DNS and the increasing phenomenon of its co-option as a new tool of global power. Building upon Internet governance scholarship and conceptual frameworks from Science and Technology Studies, the first section establishes the inherently political nature of the DNS by examining several design characteristics that shape policy challenges. These features include its hierarchical design, requirement for globally unique identifiers, finite resource pool, and its criticality and centralized role in the underlying operation of the Internet. Drawing from these characteristics, case studies are provided to suggest the following policy concerns within the DNS: name space conflicts related to speech, national

security, and property; distributional equity and individual rights issues around Internet addresses; cybersecurity challenges; privacy; and the long-simmering tensions over who should have authoritative oversight of the DNS and root zone file.

The second section of the paper examines the growing recognition of the DNS as a lever of power. We draw on primary documents from Internet governance institutions to demonstrate how the DNS is being modified or co-opted to achieve various political or economic objectives. These approaches include: domain name seizures; local DNS redirection; DNS injection; and movements to create alternate Internet roots, either emanating from activist communities, private interests, or nations outside the dominant Internet governance regime. Section three explores the implications of these approaches for network security, architectural stability, human rights, and efficacy of the Internet governance ecosystem.

The paper makes three contributions to Internet governance literature: it serves as an argument against some perceptions that the DNS is "just a technical issue"; it explicates the emerging global phenomenon of the DNS being increasingly altered or co-opted for geopolitical objectives unrelated to its underlying function; and it raises implications of these attempts to alter the DNS for the future of Internet architecture and freedom.

Public Policy Issues within the Everyday Operation of the DNS

Almost every activity online begins with a request to the Domain Name System. In terms of scope, the DNS is a broad system encompassing: the *unique name and number* identifiers for Internet-connected resources; the *distributed technological system* - databases, software, switches, protocols, and servers - responsible for resolving names into numbers, somewhat

analogous to an address book; and the *ecosystem of governing institutions* that coordinate DNS design, operation, name administration, and resource allocation.

Every device connected to the Internet is assigned a 32-bit binary identifier called an Internet Protocol (IP) address, such as 11000000010100011000001110100001, usually written in shorthand dotted-decimal notation 192.81.131.161. A unique IP address identifies the virtual location of devices or resources connected to the Internet. Humans do not necessarily use these addresses but rather more user-friendly alphanumeric domain names such as google.com or amazon.ca. A core function of the DNS is to translate between binary IP addresses computers use and text-based domain names that people use.

As a globally distributed system, the DNS is massive, resolving hundreds of billions of queries per day. The technological complexity and expansiveness of this system can obfuscate some of its underlying public interest implications. The conceptual starting point of this paper is that technologies, including Internet governance infrastructure, inherently embody values in their design, implementation and usage (Winner, 1980, Lessig, 1999, Zittrain, 2008, Author, 2009, Gillespie, 2010). Much scholarship already addresses the public interest issues implicated across layers of Internet governance systems (Goldsmith and Wu, 2008; Mathiason, 2008; Bygrave and Bing, 2009; Weber, 2009; Mueller, 2010; Kulesza, 2012; Brousseau, 2012; MacKinnon, 2012, Author, 2014).

The coordinating functions that collectively comprise "Internet governance" include standards-setting by institutions such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), the policies of private companies such as network operators and content intermediaries, national laws within borders, international agreements, and coordination of names and numbers by global institutions such as the Internet Corporation for

Assigned Names and Numbers (ICANN), DNS registries, DNS registrars, and Regional Internet Registries, among others. There is no single system but rather an ecosystem of functions. The DNS, itself requiring a complex array of coordinating functions and institutions, is only one part of this multi-layered system of tasks that collectively keep the Internet operational.

While all technologies of Internet governance have sociopolitical implications to various degrees, this paper suggests that several design characteristics of the DNS create a particular set of intrinsic policy concerns. First, and unlike other Internet governance functions, the DNS actually embeds content. Domain names contain text (e.g. amazon.com) and therefore inherently involve conflicts over speech and property. Second, the DNS creates a hierarchical system of chokepoints capable of controlling access to content. Third, the DNS constitutes a core technology necessary for the Internet to function. Given that basic systems of commerce, social life, and politics depend upon the Internet to function, DNS stability and security is an enormous public interest concern. Fourth, the DNS involves a pool of finite resources, raising inherent issues of distributional equity and potential scarcity. Fifth, the DNS requires the use of globally unique identifiers, a technical feature providing challenges both for individual privacy, because it offers the possibility of IP addresses serving as unique personal identifiers, and for governance, because some centralized coordination is necessary to fulfill the technical requirement of uniqueness for each identifier.

These DNS design features, themselves socially constructed, create unique policy challenges. Drawing from contemporary case examples, the following sections present a framework of distinct policy concerns that arise within the DNS, including: speech rights, national security, intellectual property, distributional equality, privacy, cybersecurity, and the

geopolitical power struggle over who should be responsible for centralized coordination and oversight of the DNS.

Conflicts Related to Speech and Morality

Internet infrastructure is often viewed as neutral to the content and politics that flow over it. This can never be said about the DNS. As a namespace, it inherently contains content, leading to a number of conflicts related to speech and morality. The DNS is organized in a hierarchy, divided into virtual domains that organize collections of names reachable anywhere on the network. At the top is the root zone file, which contains a master record that maps IP addresses for each top-level domain (TLD). TLDs can be generic (.com, .org) or country-codes (.uk, .ca). Historically, the U.S. government has contracted ICANN to carry out the management of this addressing system, including the management of the root zone file and allocation of IP addresses.

One historic moral controversy over the DNS emerged during the introduction of a new .xxx generic TLD. Advocates for .xxx suggested that a circumscribed area for pornographic content could facilitate parental controls. Others approved on free speech grounds. But the U.S. DOC asked ICANN to delay the .xxx implementation after receiving nearly 6,000 letters from concerned citizens. ICANN eventually approved the .xxx TLD and registry, but this case suggests the types of free speech controversies that arise in the DNS, as well as the real and potential power of both the Commerce Department and ICANN in authorizing changes to the Internet's name system.

Similar moral debates materialized after ICANN announced a massive expansion of TLDs and received almost two thousand applications for new domains. Saudi Arabia, a country in which homosexuality is criminalized and sometimes punishable by death, objected to the .gay

TLD application, because "many societies and cultures consider homosexuality to be contrary to their culture, morality, or religion" (ICANN, 2012). Saudi Arabia and other countries also opposed the introduction of TLDs such as .sexy, .dating, .porn, .adult, and others, as well as .islam over objections to a private company operating a domain representing the worldwide Muslim community.

Control over the introduction of new domain spaces equates to control over the introduction of new speech spaces and what counts as morally acceptable within a technology that transcends national boundaries but operates in bordered areas with distinct statutory and cultural contexts.

Conflicts Related to Terrorism and National Security

National security questions similarly arise over domain name administration. Important questions include: should a terrorist organization be permitted to register a domain name; are there conditions under which a domain associated with a specific country could be withdrawn from the DNS; and are TLDs permissible tools of international sanctions or compensatory damages in lawsuits related to state-sponsored terrorism?

Country-code TLDs (ccTLDs) in particular, have become entangled in national security controversies. Country-codes are rare Internet infrastructure spaces with circumscribed geographical boundaries embedding different legal and cultural contexts. In 2010, when WikiLeaks released U.S. diplomatic cables, an American domain name service provider ceased resolving queries to the organization's .org site (wikileaks.org). WikiLeaks was able to remain online using Swiss companies and the Swiss ccTLD (.ch) at wikileaks.ch.

ccTLDs were also at the center of an international terrorism-related lawsuit. In an attempt to collect damages from Iran, North Korea and Syria, a group of injured victims of a Hamas-planned suicide bombing in Jerusalem asked ICANN to seize these countries' ccTLDs and redelegate them to the plaintiffs as compensation. A U.S. court action had awarded the plaintiffs hundreds of millions in compensation and the effort to appropriate ccTLDs was part of a protracted attempt to collect damages.

The Internet governance tradition toward country-code name spaces has favored national autonomy. ICANN was reluctant to bring these Internet governance domains into lawsuits, arguing that "ccTLDS are not property subject to attachment," are "not 'owned' by the countries to which they are assigned," and that, even if they were property, the U.S. court lacked jurisdiction and "ICANN does not have the unilateral power or authority to redelegate the ccTLDS, and doing so would interfere with contractual relationships" (ICANN, 2014). ICANN successfully resisted "seizing" ccTLDs and reassigning them as civil litigation compensation.

While there have been few similar conflicts, these incident is indicative of the types of national security controversies that arise within the DNS. A pressing geopolitical question, and one sometimes arising in debates over root zone file oversight, involves the unlikely act of withdrawing a ccTLD from the root zone file and therefore potentially separating that domain from the global Internet. This question serves as a backdrop for discussions about the reach of state-sponsored cyber-terrorism as well as control over root zone file.

Conflicts Related to Property

Because the DNS embeds content in the form of names, conflicts related to intellectual property rights have been inherent in the system since the commercialization of the Internet. Domain

name trademark disputes have been an Internet policy concern for decades. Trademarks are words (Nike), phrases (Just Do It), or symbols (the Nike swoosh) distinguishing a product, service, or company for brand and consumer protection by legally deterring counterfeit products. One complication is that domain names must be globally unique, while trademarks are sometimes unique to a country or to an industry category. For example, United Van Lines, United Airlines, and the Manchester United have their own trademarks and are not in contention in the real world while only one entity can use united.com. Questions inherently arise over entitlement to a domain name associated with competing but legitimately trademarked names. Other problems arise over bad faith trademark infringement such as "cybersquatting" (registering someone else's domain name for profit) or "typosquatting" (registering a domain name nearly identical to a trademarked name to exploit user typos or misspellings).

The expansion of TLDs initiated by ICANN in 2012 introduced many trademark-related conflicts. ICANN received nearly 2,000 proposals for new TLDs, many involving legitimately trademarked product names such as Microsoft's proposals for .xbox and .office. Many applications were duplicative, with multiple proposals to operate .app, .news, and .shop, for example.

Duplicative proposals require facilitated resolution or auctioning to meet the technical requirement of global uniqueness for every new TLD. However, this has also led to a relatively new property conflict over domain name trademarks involved contention between trademark-holding companies and territorial interests. Amazon submitted an application for the .amazon TLD, as well as others including .kindle and .shop. If granted, Amazon would have become the operator and administrator for the .amazon domain. Countries with the Amazon rainforest and Patagonia regions within their borders objected to the company's application. ICANN's

Governmental Advisory Committee advised ICANN to reject the registration of .amazon, suggesting that a private company should not gain exclusive rights over a TLD containing a named region that is a publicly important and biodiverse region and natural resource (Vargas Leon and Kuehn, 2014). ICANN ultimately rejected Amazon's application. Given the requirement of unique names and legitimately trademarked brands, these types of property-related conflicts will continue for the foreseeable future.

Number Identifiers and Distributional Equality

While previous examples addressed policy concerns around domain names, Internet numbers also create a several public interest challenges. These concerns are shaped by a combination of technological requirements: the global uniqueness of each IP address; the use of an IP address as a necessary condition for using the Internet, analogous to a physical address necessary for using the postal system; and the finite set of available numbers.

The longstanding IP address standard, IPv4, assigns 32 bits to each address, providing an address space of 2^{32}, or roughly 4.3 billion unique Internet addresses. This is an insufficient number to meet contemporary demands. A newer standard, IPv6, expands the address space exponentially but is being deployed slowly, primarily because it is not backward compatible with IPv4. The global distribution of addresses has long raised questions about distributional equity, and who is permitted to access the Internet, introduce new services, and "resell" scarce IPv4 addresses through new exchange markets.

Cybersecurity Concerns

Internet engineers designed the DNS in 1984, prior to network internationalization and in an environment characterized by trust among its users (Plante, 2004; Author, 2009, 2014). Since

then, the engineering community has had to continually enhance DNS security to protect against attacks that exploit weaknesses in DNS queries. When a user accesses content online, the DNS will query - or lookup - the location of that content on the network. Some attacks tamper with the lookup process, redirecting users to fake websites to enact censorship, fraud, or identity theft. Other types of attacks, such as Denial of Service (DDoS) attacks, disrupt Internet service by overwhelming servers with traffic from multiple sources.

The most basic DNS query is called "recursive resolving". To find content on the network, a user's device will search the DNS hierarchy for information about where it is located. If the device has previously sought this information, it will be stored in its cache - or temporary memory - designed to make future lookups more efficient. If not, a device will systematically query servers down the DNS hierarchy to find the requested information.

Internet RFCs provide a much more detailed description of the process, but recursive resolution happens in several stages: if a user wishes to access a website such as "google.com", the user's device sends a request to a root server and asks where it can find the TLD operator for .com; it then queries the top-level domain operator (in this case Verisign) to find google.com; finally, it asks the server for google.com where it can find www.google.com. Google's DNS server will report back to the user's device and direct it to where the website can be found on the network (Mockapetris, 1987a; 1987b).

Currently, there is no verification mechanism to validate the information being recursively resolved: a device will ask for the IP address associated with a website and connect automatically without verifying the response the server provides. The DNS Security Extensions (DNSSEC) was created to provide a layer of authentication in the look-up process. However, in order to secure the network, DNSSEC would have to be deployed by the root zone file, DNS

registries, registrars and other servers operating at all levels of the DNS hierarchy. As a result, the deployment of DNSSEC has been extremely slow and contentious (Kuerbus and Mueller, 2010).

Privacy Concerns in the DNS

A less known policy concern is that the design and operation of the DNS directly intersects with privacy, although in ways not necessarily visible to a user, or in a way that they can control. Because of their global uniqueness, IP addresses in combination with other information can create a record of personal information about Internet users. But DNS privacy issues go beyond the layer of names and numbers, and affect the protocols that are necessary for the resolution process. As a 2014 IETF Internet Draft warned, "Recent events have required urgent consideration of privacy concerns in Internet protocols... the lack of confidentiality controls in the DNS protocol is of considerable concern" (Hallam-Baker, 2014).

One DNS privacy concern involves the confidentiality of DNS queries. When an end-user searches for information online, the DNS query is almost always unencrypted. As explained in an informational RFC draft, "All this DNS traffic is today sent in clear (unencrypted), except a few cases when the IP traffic is protected, for instance in an IPsec VPN." (Bortzmeyer 2015: 1). A user's DNS requests can reveal, among other things, websites the user visits, raising important privacy concerns for how these queries might be processed, retained, or shared.

Another distinct concern is the privacy of domain name registrants. The WHOIS protocol, described in Internet RFCs in 1982, required anyone with a host name to register their real name, address, and other personal information, although subsequent services have arisen for those wishing to anonymize domain name registrations (Daigle, 2004). Law enforcement agencies frequently use IP addresses to track online criminals. However, an evolving policy

question at the intersection of individual privacy and law enforcement remains: should it be legally permissible for domain name registrants to remain anonymous?

Tension over the Root Zone File

Since the Internet's inception, there have been central systems for allocating Internet names and numbers to ensure global uniqueness of each identifier. This centralized coordination is necessary but has contributed to the historic geopolitical power struggle over DNS oversight.

Because of the trajectory of the Internet originating in the United States with Department of Defense funding, the US government has historically retained a role in oversight of critical Internet resources. A 1998 a memorandum of understanding between ICANN and the US DOC initiated a process of internationalization and commercialization that transitioned DNS coordination functions to ICANN, while retaining accountability to the US government. A second contract between the DOC and ICANN authorized the Internet Assigned Numbers Authority (IANA) to become a subsidiary body of ICANN contracted to perform various technical functions.

The US government's contractual relationship with ICANN and its role in authorizing changes to the root zone file have long been contentious issues. Attempts to transition US oversight of names and numbers to the international community date back to the World Summit on the Information Society in Geneva in 2003 and in Tunis in 2005. The formation of the United Nations Internet Governance Forum was a compromise designed to continue the dialogue about how to internationalize these functions. In 2011, in the context of ongoing international concern, the US government awarded the IANA contract to ICANN for up to an additional seven years.

In the aftermath of disclosures about expansive US government surveillance practices, concerns about exclusive US oversight of IANA and control over the root zone file escalated. Global tensions over the root predate more recent concerns about government surveillance, and also have no direct relationship with it. Nevertheless, concern about NSA surveillance practices have created a loss of trust in the stewardship and unique relation of the US government in other areas related to Internet governance, and have heightened the already entrenched interest in continuing to internationalize ICANN and control of other critical Internet resources (Author et al., 2015). In March 2014, the NTIA announced that the United States would transition oversight of the IANA function to the multistakeholder community by September 2015. At the time of writing, proposals for replacing the current model exist and the US Government's deadline for the transition is set to expire soon.

Co-opting DNS Infrastructure

A primary argument of this paper is that the DNS is not only political in its day-to-day operation, but is increasingly recognized as a proxy site for extraneous geopolitical power. The very technological attributes that have shaped the public-policy issues embedded in DNS operation have attracted increasing interest in the ability of the DNS to control the flow of information, enforce content-related laws, or enact censorship. Distinct from the policy issues arising in its operation and oversight, the DNS has increasingly been politicized for purposes unrelated to its coordination or administration. Some of these approaches rely upon altering the underlying technical architecture of the DNS while others seek modifications to the system of administration that keeps the Internet operational. This section examines four distinct alterations: 1. domain

name seizures; 2. local DNS redirection; 3. DNS injection; and 4. movements to create alternate Internet roots.

Domain Name Seizures

Law enforcement has turned to the DNS as an intervening tool to address piracy. Intellectual property rights enforcement online has historically targeted individuals involved in infringement or the infringing content itself, such as a YouTube video, or relied upon digital rights management technologies. The DNS has emerged as a tool for redirecting access to websites selling counterfeit goods or illegally sharing copyrighted movies, games, or songs.

Domain name seizures involve removing DNS data from a registry or the operator of an authoritative name server. When registries or operators are lawfully subject to comply with domain name seizures, they will either completely remove the domain name from their database, or redirect the user to a law enforcement notice (SSAC, 2012).

In the United States, domain name seizures are carried out by the US immigration and Customs Enforcement (ICE) arm of the Department of Homeland Security. ICE began using domain name seizures to shut down websites geared toward counterfeit trafficking and piracy in 2010. However, law enforcement agencies can only seize domains that are registered with a registrar, registry or operator that is located within their national jurisdiction. To broaden legal reach, organizations such as ICE also partner with law enforcement agencies in other countries such as EUROPOL in the European Union (Daigle, 2015).

To avoid seizures, some website owners have begun registering domain names with a registrar located in a more permissive legal jurisdiction. For example, online gambling or file-sharing websites are often located in countries that do not have strict legal prohibitions or enforcement norms. To seize infringing websites whose domain name registrars are located

overseas, there has been a growing trend by the U.S. government to address this infringement by approaching American registry operators. In 2012, Homeland Security seized an online gambling website - bodog.com - that was registered in Canada. In order to circumvent the jurisdictional issues, Homeland Security obtained a warrant that ordered American-based TLD operator Verisign to redirect users to a law enforcement notice (Geist, 2012). This example raises important questions over US jurisdictional oversight of the DNS as many key TLD operators are based in the US (Kravets, 2012).

Domain name seizures also raise questions about collateral effects on freedom of expression and erroneous over-blocking. A blocked domain name could remove access to lawful material, as well as infringing content. To use an extreme example for emphasis, it would be excessive to block all of youtube.com because it contains a subset of infringing content. Further, domain name seizures often do not provide the owner sufficient time and resources to challenge seizures, leaving room for erroneous or malicious blocking (Seltzer, 2011). Finally, the efficacy of DNS seizures for intellectual property enforcement remains unclear because content can so easily rematerialize on a different website.

Local DNS Redirection

A form of domain name redirection that raises similar concerns but also "tampers" with the universal consistency of the DNS is local redirection, the imposition of restrictions on a non-authoritative DNS operator, such as an ISP, that is physically located within a national jurisdiction. Typically, it requires a user's ISP to ignore the universally consistent DNS record and redirect a particular DNS lookup, so when a user attempts to access a website, the DNS server would return the address of another website, or the lookup would fail all together.

Local redirection has become a common technique for governments to locally block content such as pirated material or politically objectionable speech. American policymakers 2010 attempt to curb online piracy through the proposed Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA) would have required ISPs to locally redirect DNS lookups for sites that were believed to contain content that violated intellectual property rights.

Other governments use local redirection to block social media and other content. In March of 2014 the Turkish government used local redirection to Twitter and YouTube within the country (Tuysuz and Watson, 2014). Later that year, the Iraqi government ordered its Ministry of Communications to block Twitter, Google, YouTube and Facebook in response to civil unrest (Miller, 2014). Local redirection has also been used to ban Twitter in Iran in 2009 (Sheikholeslami, 2009) in South Korea in 2010 (Harlan, 2010) and in Egypt in 2011 (Siegler, 2011).

Locally redirecting traffic can problematically affect the functionality and universality of the Internet. Authoritative records are passed down through the DNS hierarchy from registries to ISPs. If an ISP changes the authoritative record locally, the principles of universality and consistency in the DNS lookup process is violated, as the database used by the ISP would not match the authoritative record (Author, 2012).

Local redirection does not always stay local but can have cascading consequences for the entire network (Daigle, 2015). In 2008 the Pakistan government ordered Pakistani Telecom to block YouTube by redirecting local traffic away from the website. Pakistan Telecom complied by redirecting Internet users to a page indicating that YouTube had been blocked. However, the routing information uploaded by Pakistani Telecom was passed up the DNS hierarchy until

everyone who tried to access YouTube, regardless of their country, was directed to the Pakistan network block (Singel, 2008).

Local redirection can also harm DNS security and the use of the DNSSEC protocol. DNSSEC attaches a cryptographic signature to authoritative records, providing a layer of authentication in the lookup process so that users can confirm whether information a server returns is correct. If an ISP changes the authoritative record locally, DNSSEC would be unable to distinguish between the redirection and other more malicious actions that divert users to fake websites. In a technical paper on the security concerns raised by PIPA and local redirection, Internet pioneer Steve Crocker and colleagues (2011: 2) wrote that local redirection would "enshrine and institutionalize the very network of manipulation that DNSSEC must fight in order to prevent cyberattacks and other malevolent behaviour on the global Internet, thereby exposing networks and users to increased security and privacy risks." While intellectual property enforcement is an important objective, the use of the DNS to achieve this goal raises serious technical and security concerns.

DNS Injection Techniques

One of the more malicious techniques for co-opting the DNS to achieve political or economic goals involves exploiting weaknesses in its design. DNS injection techniques are technical alterations that disrupt the resolution process and divert Internet traffic away from legitimate websites. Typically, these techniques will cause DNS servers to lie about associated IP addresses, names, the authoritative servers for the domain, or any combination thereof (Lowe, Winters and Marcus, 2007).

So-called "man-in-the-middle" techniques monitor DNS requests and inject false information into the resolution process. Cybercriminals often use these techniques to redirect

users to fake websites - such as a fake bank or email login page - to collect personal or financial information from victims. They are also used by states to achieve goals such as content control. The Great Firewall of China is known to use injection techniques to censor and block content (Lowe et al., 2007; Zittrain and Edelman, 2003).

In addition to politically motivated exploitations to the DNS resolution process, private companies have also been known to inject misinformation to achieve economic goals. ISPs or content providers that engage in online advertising or data collection will often hijack DNS queries and redirect users to an intermediate "loading" webpage that displays advertisements (Metz, 2009) and/or installs cookies to collect user data (McMillan, 2014) before the user is directed to their requested content.

Injection techniques create risks within the complex technical system that is the DNS. If a query is injected with a false response, and a server accepts the fake record, the server's cache becomes "poisoned" and subsequent queries are answered with the false information. While DNS poisoning most often has local effects in its redirection, it can also have global implications. In 2010, an ISP outside of China mistakenly configured its DNS servers to fetch information from DNS servers in China and cached them on its own servers. Other ISPs fetched this information and used it on their servers, poisoning entries until a number of US residents were blocked from accessing popular social media websites from their American ISP (McMillan, 2010).

Alternate Roots

A variety of political and economic motivations have also led to controversial attempts to introduce alternative roots to operate independently from the universal DNS hierarchy and

ICANN's root zone file. Instead, they provide independent root name services and other TLD name system management functions (SSAC, 2006). Some alternate roots exist simply to promote privacy and security. For example, corporations often operate private intranets to keep sensitive information off the public Internet. Engineers often create alternate roots to analyze new technology and study its impact on the current system. Outside of these private naming systems and experimental uses, attempts to create alternate roots have a range of economic and political motivations.

Market-based incentives for alternate roots date back to the late 1990s when the Internet's potential for economic growth and commercialization became evident. Alternate roots establish their own root and TLD naming services without forming an official relationship with ICANN. When these alternatives emerged, commercial TLD administrators claimed that they were a "lucrative business opportunity" (SSAC, 2006: 8). However, Mueller (2001: 2) suggests that additional roots may have been caused by "ICANN's extremely restrictive and slow addition of new top-level domains to the domain name system."

In response to increasing corporate demand for new generic TLDs, ICANN eventually approved the creation of new gTLDs for brands and organizations. Beginning in 2011, anyone willing to pay an application fee of US$185,000 could apply for a new TLD. However, a number of alternate root and TLD naming providers still exist and operate under a variety of business models (SSAC, 2006). Many of these providers offer cost-efficient options for organizations who cannot afford to pay ICANN's gTLD application fee.

Noncommercial alternate roots have also emerge, primarily in situations in which individuals or organizations are unsatisfied with the established TLD name system or its administration. Reasons for operating these types of alternate roots can include restricting

membership, expressing political or social activism, or carrying out illegal activities online (SSAC, 2006).

In 2010, when the US government began to aggressively enforce intellectual property rights online, discussions about a new competing root server where pirated material could be shared began taking place across the Web. Calls for a decentralized, peer-to-peer system where users would run segments of the DNS on their own computers spread across the Internet, so that if a domain was blocked by a registry, users could still access it (Musiani, 2012).

Dissent-based alternatives have also been used as a way for citizens and organizations to bypass state censorship and bolster anonymity online. The Tor exit-relay is the most popular alteration that routes DNS queries through a series of servers to enhance anonymity online. Tor was originally designed by the US Naval Research Laboratory to secure sensitive military communications. However, it is increasingly used by individuals to protect anonymity online, or to access the dark web and carry out illegal activity. A recent study found that most of the hidden content on the dark web are dedicated to selling illegal drugs, and that most of the traffic on the network go to websites containing child sexual abuse (Ward, 2014).

Geopolitically motivated alternatives are operated by state actors who seek to control and regulate online content. These types of alternatives give states full control of content on the Internet for users in the country, as well as who and how it can be accessed. Examples include states such as North Korea (Grothaus, 2014) and Iran (Ungerleider, 2012), which have created their own private intranets to censor and control all the content available to citizens in their respective countries.

In 2012 China put forward a proposal in the form of an IETF working paper to make it easier for countries to create independent root servers, suggesting that the DNS is “not suitable to

autonomy and scalability and can't keep up with the fast development of the Internet" (Diao and Lia, 2012: 3). Russia has also begun experimenting with this governance by infrastructure trend. In 2014, officials noted that they were experimenting with ways to break away from the centralized ICANN system (Anishchuk, 2014).

Alternate roots as a form of governance by infrastructure have also arisen in the context of multilingual names in TLD labels. Technically speaking, the IETF developed multilingual standards as early as 1997 (Klensin, 2005), but ICANN was slow to implement them. In 2005-2006, China began experimenting with multilingual Chinese-character gTLDs for .china 中国 .company 公司 and .net 网络 (MacKinnon, 2006). There were also reports that other countries, such as Iran, Saudi Arabia and Egypt, were considering taking similar steps if ICANN did not respond to the language and access barriers their countries were facing (Marsan, 2006). Because of the mounting pressure, ICANN began experimenting with internationalized domain names and approved a fast-track process in October 2009 (ICANN, 2009).

Alternate roots can interact with ICANN's root in a number of ways (Higgs, 2001; Mueller, 2001). Alternate roots are separate from ICANN's DNS hierarchy, and users can only access content on alternate roots if they voluntarily set their resolvers to access alternate DNS servers. Because the systems are completely separate, the universality of the Internet will always be impacted. It is important to note fragmentation due to alternate naming systems can have some positive effects, such as protecting sensitive data and personal information from security breaches, improving connection speeds, and implementing parental controls. Moreover, unlike many default servers, popular alternative servers like OpenDNS and Google Public DNS support DNSSEC.

However, the importance of a single DNS root has long been debated by the Internet community (IAB, 2000). The fundamental design goal of the DNS is to provide unique and stable names for critical Internet resources. If duplicate domain names are created, the DNS will no longer be able to resolve names into IP addresses. As Stuart Lynn (2001) president of ICANN stated at the time:

> To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority.

Separate from the issue of universality, is the interoperability of the network. When conflicting or duplicative names are assigned, the principle of interoperability is violated. It is for this reason that much of the Internet community has advocated for a single, globally consistent root. In order to avoid assigning duplicate domain names, some alternate root administrators will provide name resolution services for their alternative root and naming systems, as well as TLDs resolved by ICANN, which appends their own root zone file to the root zone file published by IANA (Higgs, 2001; SSAC, 2006). However, this does not guarantee that all the TLDs published in every single alternate root as well as the authoritative are coordinated to ensure there is no overlap in name assignments. Moreover, there are currently no other mechanisms or technical ways of ensuring the coordination of all alternate root and name system operators (SSAC, 2006).

The Stability of Internet Governance Depends on the Future of the DNS

The intrinsic policy dimensions of the DNS and the increasing turn to this system as a proxy for broader geopolitical conflict underscore that DNS design and administration is not merely a technical issue. The DNS is recognized as a powerful source of control over content and of the

Internet infrastructure necessary to sustain basic systems of commerce and culture. The rationales for co-opting or altering the DNS are diverse:

- Content control - including intellectual property rights enforcement and censorship;
- Cybercrime - such as using DNS injection techniques for financial fraud;
- Revenue generation - such as delivering online ads;
- Geopolitical power - such as real and symbolic power struggles over the root zone file;
- Dissent - such as activists circumventing dominant modes of infrastructure and governance.

This turn to the DNS is not an isolated phenomenon but part of a broader recognition of Internet governance infrastructure as a site of global power. Other examples include three-strike laws that block Internet access after repeated instances of copyright infringement; the use of deep packet inspection for capturing user preferences or enacting surveillance; or the resurgence of proprietary technical standards as trade barriers.

Because the DNS has worked well historically, it is easy to take for granted its ongoing operational stability. The case studies herein suggest that the increasing DNS politicization raises troubling implications that could potentially destabilize systems of Internet governance. One concern is Internet fragmentation. Three of the four DNS interventions described in this paper raise the possibility of transforming the DNS from a universally consistent system to one that varies based on geography, constituency or technology. Domain name seizures, despite other potential problems, at least retain a globally consistent DNS registry system. This is not the case with local DNS redirection, alternate roots and DNS injection techniques, which violate the principle of universality in DNS lookups. Given the scale and importance of the DNS,

movements away from universality, towards fragmentation, will change the historic norms of the Internet and potentially destabilize the central systems keeping the Internet operational.

Concerns about fragmentation are closely related to concerns about stability and reliability. Three of the DNS interventions described in this paper impact the stability and consistency of the DNS lookup process. Local DNS redirection, alternate roots and DNS injection techniques change the content and therefore quality of authoritative records, impacting the consistency of lookups, historically imbued in the DNS.

A third concern is security. The DNS is vulnerable to a number of attacks with significant potential effects on Internet security and the trustworthiness of the resolution process. Protocols exist to mitigate these vulnerabilities but deployment has been slow and has raised complex Internet policy questions. Additionally, policies designed to mitigate certain problems, such as piracy, can have Internet security repercussions, such as the suggestion of local DNS redirection for intellectual property rights enforcement. This points to a larger challenge within the Internet governance space. Policymakers do not necessarily understand the complex technical underpinnings that maintain Internet stability and security.

A fourth destabilizing concern relates to human rights. The DNS interventions described in this paper can all be used to block or censor content or otherwise limit digital expression. The Internet's core technical design is agnostic to the content flowing across it and who or what is connected at endpoints. DNS interventions that block the flow of information violate this principle, and can create collateral damage to the broader Internet, limiting an individual's ability to access information or express oneself. Creating normative structures around content redirection can also diminish a country's ability to participate in the global economy.

A final concern relates to the efficacy of the Internet governance ecosystem as a whole. The politicization of infrastructure is increasing tension over control of Internet governance institutions and arrangements that keep the Internet operating. Geopolitical tensions will only increase as states increasingly recognize the DNS as a site of power and struggle to regulate a technology that spills over into every aspect of political, social and economic life. No matter how these geopolitical struggles resolve, as goes control of the DNS, so goes control of the Internet.

References

Anishchuk A (2014) Russia eyes measures to fend off Western Internet Threat: Kremlin. *Reuters Magazine*, 19 September. http://www.reuters.com/article/2014/09/19/us-russia-internet-idUSKBN0HE1F320140919

Author (2009).

Author (2012).

Author (2014).

Author, Author, Hampson F, Jardine E, and Raymond M (2015).

Bortzmeyer S (2015) IETF Draft, DNS Privacy Considerations. https://tools.ietf.org/html/draft-ietf-dprive-problem-statement-01

Brousseau E, Marzouki M and Méadel C, eds (2012). *Governance, Regulation, and Powers on the Internet.* Cambridge: Cambridge University Press.

Bygrave LA and Bing J, eds (2009) *Internet Governance: Infrastructure and Institutions.* Oxford: Oxford University Press.

Crocker S, Dagon D, Kaminsky D, McPherson, D, and Vixie P (2011) Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the Protect IP Bill. http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf

Daigle L (2004) WHOIS Protocol Specification. RFC 3912

Daigle L (2015) On the Nature of the Internet. *Global Commission on Internet Governance Paper Series: No. 7.*

Diao Y and Lia M (2012) DNS Extension for Autonomous Internet (AIP). IETF Internet Draft. https://tools.ietf.org/html/draft-diao-aip-dns-00

Geist M (2012) Bodog.com case sends warning to all Canadian websites: Geist. *The Star*, 3 March. http://www.thestar.com/business/2012/03/03/bodogcom_case_sends_warning_to_all_canadian_websites_geist.html

Gillespie T (2010) The politics of platforms. *New Media & Society*, 12(3) 347-364.

Goldsmith J and Wu T (2008). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Grothaus M (2014) What It's Like To Use North Korea's Internet. *Fast Company*, September 24 http://www.fastcolabs.com/3036049/what-its-like-to-use-north-koreas-internet

Hallam-Baker P (2014, November 7) Internet-Draft expiring May 11, 2015, "DNS Privacy and Censorship: Use Cases and Requirements."

Harlan C (2010) South Korea tries to block Twitter Messages from North. *Washington Post*, 21 August http://www.washingtonpost.com/wp-dyn/content/article/2010/08/20/AR2010082005741.html

Higgs S (2001) Alternate roots for domain names explained in IETF draft. *Politech: Politics & Technology*. http://www.politechbot.com/p-02077.html

IAB (2001) IAB Technical Comment on the Unique DNS Root. https://www.ietf.org/rfc/rfc2826.txt

ICANN (2009) Internationalized Domain Names. https://www.icann.org/resources/pages/idn-2012-02-25-en

ICANN (2012) New Generic Top-Level Domains-Application Comment Details https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/6191

ICANN (2014) “Motion to Quash Writ of Attachment” in the U.S. District Court for the District of Columbia, filed July 29, 2014. www.icann.org/.../ben-haim-motion-to-quash-writs-1-29jul14-en.pdf

Kravets D (2012) Uncle Sam: If It Ends In .com It’s .seizable. *Wired Magazine*, 6 March http://www.wired.com/2012/03/feds-seize-foreign-sites/

Klensin J (2005) National and Local Characters for DNS Top Level Domain (TLD) Names. RFC 4185

Kulesza J (2012) *International Internet Law*. New York: Routledge.

Kuerbis B and Mueller M (2010) Securing the Root. In: *Opening Standards: The Global Politics of Interoperability*. Author (ed). The MIT Press: Cambridge, MA.

Lessig L (1999) *Code and Other Laws of Cyberspace.* New York: Basic Books.

Lowe G, Winters P, and Marcus ML (2007) The Great DNS Wall of China. https://cs.nyu.edu/~pcw216/work/nds/final.pdf

Lynn S (2001) Discussion Draft: A unique Authoritative Root for the DNS. http://archive.icann.org/en/meetings/stockholm/unique-root-draft.htm

MacKinnon R (2012) *Consent of the networked: The worldwide struggle for Internet freedom.* New York, NY: Basic Books.

McMillan R (2010) China’s Great Firewall Spreads Overseas. *Computer World*, 25 March http://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html

McMillan R (2014) Verizon’s Perma-Cookie Is a Privacy Killing Machine. *Wired Magazine*, 27 October http://www.wired.com/2014/10/verizons-perma-cookie/

Marsan CD (2006) Native Language Domains Threaten 'Net. *NetworkWorld*, 27 March http://www.networkworld.com/article/2310065/lan-wan/native-language-domains-threaten--net.html?page=1

Mathiason J (2008). *Internet Governance: The New Frontier of Global Institutions.* New York: Routledge.

Metz C (2009) Comcast Trials Domain Helper Service DNS Hijacker Here to Stay. *The Register*, 28 July

Miller J (2014) Iraq Blocks Facebook and Twitter in bid to Restrict Isis. *BBC News*, 26 June

Mockapetris P (1987a) Domain Names - Concepts and Facilities. RFC 1034

Mockapetris P (1987b) Domain Names - Implementation and Specification. RFC 1035

Mueller M (2001) Competing DNS Roots: Creative Destruction or Just Plain Destruction? http://arxiv.org/ftp/cs/papers/0109/0109021.pdf

Mueller M (2010) *Networks and States: The Global Politics of Internet Governance.* Cambridge: MIT Press.

Musiani F (2012) A Decentralized Domain Name System? User-Controlled Infrastructure as Alternative Internet Governance. http://web.mit.edu/comm-forum/mit8/papers/Musiani_DecentralizedDNS_MiT8Paper.pdf

Plante NA (2004). Practical Domain Name System Security: A survey of Common Hazards and Preventative Measures. http://www.infosecwriters.com/text_resources/pdf/dns-security-survey.pdf

SSAC (2006) Alternative TLD Name Systems and Roots: Conflict, Control and Consequences. https://www.icann.org/en/system/files/files/alt-tlds-roots-report-31mar06-en.pdf

SSAC (2012). SSAC Advisory Impacts of Content Blocking via the Domain Name System.

https://www.icann.org/en/system/files/files/sac-056-en.pdf

Seltzer W (2011) Exposing the Flaws of Censorship by Domain Name. Secure Systems, *IEEE Security & Privacy*. http://wendy.seltzer.is/writing/COICA-IEEE.pdf

Sheikholeslami A (2009) Iran Blocks Facebook, Twitter Sites Before Elections. *Bloomberg*, 23 May http://www.bloomberg.com/apps/news?pid=newsarchive&sid=anh.uW3gNZp4

Siegler MG (2011) Twitter Confirms That They're Being Blocked in Egypt. *TechCrunch*, January 25. http://techcrunch.com/2011/01/25/twitter-blocked-in-egypt/

Singel R (2008) Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net. *Wired Magazine*, 25 February http://www.wired.com/2008/02/pakistans-accid/

Steinhoff U, Wiesmaier A and Arauko R (2006) State of the Art in DNS Spoofing. https://www.cdc.informatik.tu-darmstadt.de/~rsa/papers/DNS-spoofing-ACNS2006.pdf

Tuysuz G and Watson I (2014) Turkey blocks YouTube days after Twitter Crackdown. *CNN*, 27 March http://www.cnn.com/2014/03/27/world/europe/turkey-youtube-blocked/

Ungerleider N (2012) Iran's "Second Internet" Rivals Censorship of China's "Great Firewall" *Fast Company*, 23 February

Vargas Leon P and Kuehn A (2014) The Battle for Critical Internet Resources: South America vs. Amazon. 9th Annual Conference of the Global Internet Governance Academic Network, Bali Indonesia.

Ward M (2014) Tor's most visited hidden sites host child abuse images. *BBC News Technology*, 30 December http://www.bbc.com/news/technology-30637010

Weber R (2009) *Shaping Internet Governance: Regulatory Challenges.* Springer.

Winner L (1980) Do artifacts have politics? *Daedalus*, 109(1), 121-136.

Zittrain J and Edelman B (2003) Internet Filtering in China. *IEEE Internet Computing*. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf

Zittrain J (2008). *The Future of the Internet and How to Stop it*. New Haven: Yale University Press.