Article

new media & society
2018, Vol. 20(1) 332–350
© The Author(s) 2016
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1461444816662932
journals.sagepub.com/home/nms
SAGE

The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom

Samantha Bradshaw
Centre for International Governance Innovation, Canada

Laura DeNardis
American University, USA

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 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 phenomenon involves governmental and private forces increasingly altering or co-opting the DNS for political and economic purposes distinct from its core function of resolving Internet names into numbers. This article examines both the intrinsic politics of the DNS in its operation 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, architectural stability, and the efficacy of the Internet governance ecosystem.

Keywords

Alternate roots, cybersecurity, domain name seizures, Domain Name System, freedom of expression, IANA, ICANN, intellectual property rights, Internet governance, privacy

Corresponding author:
Samantha Bradshaw, Centre for International Governance Innovation, 67 Erb Street West, Waterloo, ON N2L 6C2, Canada.
Email: sam.r.bradshaw@gmail.com

Introduction

Control over the Internet's Domain Name System (DNS) has been one of the most contentious policy challenges of our time. The DNS is at the center of numerous political issues, ranging from government surveillance to economic concerns around the distribution of pirated movies or the sale of pharmaceutical products online. Internet security and stability are other battle fronts, as the DNS is increasingly used as an attack vector or a chokepoint for censorship. There is also longstanding discord over the historic involvement of the US Department of Commerce (DOC) in overseeing aspects of DNS administration.

Because the DNS performs a straightforward function of resolving Internet domain names into numerical identifiers, many have described aspects of its oversight as a "clerical" or "merely technical" task (National Telecommunications and Information Administration [NTIA], 2014). This type of rhetorical framing can serve to mask or minimize the DNS' policymaking functions. Far from being merely a technical task, DNS design and administration implicate public interest concerns such as trademark disputes, infrastructure stability and security, resource allocation, and free speech.

While these are important policy issues with implications for commerce, human rights, and Internet stability, there is also a parallel but distinct phenomenon in which governmental and private forces are increasingly turning to the DNS for political or economic purposes separate from its core functions. This phenomenon can be referred to as the "turn to infrastructure" in Internet governance (DeNardis, 2012).

This article fills a gap in the 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 "Public policy issues within the everyday operation of the DNS" section establishes the inherently political nature of the DNS by examining several design characteristics that shape policy challenges, such as its hierarchical design, requirement for globally unique identifiers, finite resource pool, criticality, and centralized role in the underlying operation of the Internet. Drawing from these characteristics, specific examples are provided to suggest the following policy concerns within the DNS: name space conflicts related to speech, language, national security, and property; distributional equity and individual rights issues around Internet addresses; cybersecurity challenges; privacy; and tensions over DNS and root zone file oversight.

The section "Co-opting DNS infrastructure" of this article examines the growing recognition of the DNS as a lever of power (Mueller and Van Eeten, 2013). We draw on primary documents from Internet governance institutions to demonstrate how the DNS is being modified or co-opted to achieve goals. These approaches include the following: 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. The section "Internet stability and freedom depend on the DNS" explores the implications of these approaches for network security, architectural stability, human rights, and the efficacy of the Internet governance ecosystem.

This article has three implications for Internet governance scholarship and policy: it serves as an argument against 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 DNS. In terms of scope, the DNS is a broad system encompassing the following: 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, administration, and resource allocation.

Every device connected to the Internet is assigned a 32-bit (or 128-bit) 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 resources connected to the Internet. Humans often use a more user-friendly alphanumeric domain name such as google.com or amazon.ca. The DNS translates between 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 article is that technologies, including Internet governance infrastructure, inherently embody values in their design, implementation, and usage (Braman, 2012; DeNardis, 2009; Gillespie, 2010; Lessig, 1999; Winner, 1980; Zittrain, 2008). Much scholarship already addresses the public interest issues embedded within layers of Internet governance systems (Brousseau et al., 2012; Bygrave and Bing, 2009; DeNardis, 2014; Goldsmith and Wu, 2008; Kulesza, 2012; MacKinnon, 2012; Mathiason, 2008; Mueller, 2010; Weber, 2009).

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, laws, international agreements, and the coordination of names and numbers by global institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN), DNS registries, 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, several design characteristics of the DNS create a particular set of policy concerns. First, unlike other Internet governance functions, the DNS actually embeds content. Domain names contain text and therefore inherently involve conflicts over speech, language, 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, DNS stability and security is an enormous public interest concern. Fourth, the DNS involves a pool of finite resources, raising 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 design features, themselves socially constructed, create unique policy challenges. Drawing from contemporary real-world examples, the following sections present a framework of distinct policy concerns that arise within the DNS, including the following: speech rights and morality, terrorism and national security, language and internationalization, property, distributional equality, cybersecurity, privacy, and the geopolitical power struggle over the 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 name space, it inherently contains content, leading to a number of conflicts related to speech. The DNS is organized hierarchically, divided into virtual domains that organize collections of names reachable anywhere on the network. At the top is the root zone file containing a master record mapping IP addresses for each top-level domain (TLD). TLDs can be generic (.com and .org) or country-codes (.uk and .ca). Historically, the US 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 early controversy emerged during the introduction of a new .xxx generic TLD. Advocates for .xxx suggested that a confined area for pornographic content could facilitate parental controls. Others approved on free speech grounds. But the US Commerce Department asked ICANN to delay the .xxx implementation after receiving nearly 6000 letters from citizens concerned about the effect a circumscribed area for pornography would have on the society. 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 2000 applications for new domains. Saudi Arabia, a country in which homosexuality is criminalized and sometimes punishable by death, registered objections 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 .sexy, .dating, .porn,

.adult, and .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 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 also sometimes arise over domain name administration such as the following: 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? 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 enmeshed in national security issues. In 2010, when WikiLeaks released US diplomatic cables, an American domain name service provider ceased resolving queries to the organization's .org site (wikileaks.org). WikiLeaks remained online using Swiss companies and the Swiss ccTLD (.ch) at wikileaks.ch.

ccTLDs were also at the center of an international terrorism-related lawsuit. Seeking 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 US 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 (ICANN, 2014).

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 a property, the US 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 incidents implicate the types of national security controversies arising within the DNS. One geopolitical question 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 the root zone file.

Conflicts related to language and internationalization

Other types of domain name controversies have arisen because of language barriers, both in terms of participation in institutions and in access to domain names in native language scripts. The work of institutions setting standards related to the DNS (e.g. the IETF and the W3C) or coordinating names and numbers (ICANN) is done primarily in English. Even in organizations that have completely open norms of participation and informational transparency, this language barrier has inherently reduced participation for non-English speakers.

Another language barrier has been embedded within domain names themselves. Until the early 21st century, domain names were only available in the Latin alphabet, precluding the use of languages employing Arabic, Chinese, Cyrillic, or other scripts. Native languages in China, Eastern Europe, Japan, Korea, the Middle East, and elsewhere were not able to be included in the DNS. As the Internet expanded internationally, this constraint became an obvious barrier to participation and the Internet technical community began developing standards to incorporate non-Latin scripts in domain names and TLDs (see Fältström et al., 2003; ICANN, 2009). While residual technical constraints to full language inclusion have continued, as well as lack of full universal acceptance of internationalized domain names, the multilingual script expansion of domain names has helped internationalize the Internet.

Conflicts related to property

Because the DNS includes names, conflicts related to intellectual property rights (especially domain name trademark disputes) have been inherent in the system since the Internet's commercialization. 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 industry category. For example, United Van Lines, United Airlines, and the Manchester United operate simultaneously in the real world while only one entity can use united.com. Questions 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).

For resolving global disputes over domain name trademarks, ICANN adopted the Uniform Domain Name Dispute Resolution Policy (UDRP) (ICANN, 1999). All ICANN-accredited domain name registrars in generic TLDs (e.g. .com, .net) agree to adopt the UDRP as a policy, which requires a domain name registrant to warrant that the selected name does not infringe trademark rights and which creates a mechanism for arbitration and expedited review via an approved dispute–resolution service provider (such as the World Intellectual Property Organization).

The expansion of TLDs initiated by ICANN in 2012 introduced many trademark-related conflicts. ICANN received nearly 2000 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 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

Internet numbers also create 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, Internet Protocol version 4 (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 (DeNardis, 2009). 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 exchange markets. Future innovations related to the Internet of Things also raise new policy concerns, as the networking of billions of new devices straining the IP address space, possibly even in the realm of IPv6.

Cybersecurity concerns

Internet engineers designed the DNS in 1984, prior to Internet internationalization and in an environment characterized by trust among its users (DeNardis, 2009, 2014; Plante, 2004). 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 Distributed Denial of Service (DDoS) attacks, disrupt 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 within the DNS hierarchy to find the requested information.

Internet Requests for Comments (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 TLD operator (in this case Verisign) to find google.com; finally, it asks the server for google.com where it can find http://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).

Historically, there has been no verification mechanism to validate the information being recursively resolved; a device will request the IP address associated with a website and connect automatically without verifying the response the server provides. The DNS Security Extensions (DNSSEC) protocol suite was created to authenticate this lookup process. However, to secure the network, DNSSEC would have to be deployed by the root zone file, DNS registries, registrars, and other servers at all levels of the DNS hierarchy. As a result, the deployment of DNSSEC has been slow and sometimes contentious (Kuerbis and Mueller, 2011).

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 neither visible nor controllable by users. As a 2014 IETF Internet Draft suggested, “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, the DNS query is almost always unencrypted. As explained in an informational RFC, “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). Users’ DNS requests can reveal, among other things, websites they visit, raising privacy concerns regarding how these queries might be processed, retained, or shared.

Another 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 as follows: should it be legally permissible for domain name registrants to remain anonymous to the broader Internet public?

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. This centralized coordination has contributed to the historic and geopolitical power struggle over DNS oversight.

Because the Internet originated 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 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 at least to the World Summit on the Information Society in Geneva in 2003 and Tunis in 2005. The formation of the United Nations Internet Governance Forum was a compromise designed to continue the dialog 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 7 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 correlation. Nevertheless, concern about National Security Agency (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 (Bradshaw et al., 2015). In March 2014, the NTIA announced that the United States would transition oversight of the IANA function to the multi-stakeholder community by September 2015. In 2016, a proposal for replacing the current model was put forward by the Internet community, but at the time of writing, the resolution is still pending due to issues around accountability within ICANN.

Co-opting DNS infrastructure

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 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. 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. Historically, intellectual property rights enforcement online has targeted individuals involved in infringement or the infringing content itself or relied upon digital rights management technologies. However, the DNS has emerged as a tool for enforcing property rights by redirecting access to websites selling counterfeit goods or illegally sharing copyrighted materials.

Domain name seizures are used to remove DNS data from a registry or the operator of an authoritative name server. When registries or operators are lawfully subject to comply with 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 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 within their national jurisdiction. To broaden legal reach, organizations such as ICE also partner with law enforcement agencies in other countries such as European Police Office (EUROPOL) in the European Union (Daigle, 2015).

To avoid seizures, some website owners register domain names with a registrar located in a more permissive legal jurisdiction. However, there has been a growing trend by the US government to approach American-based registry operators in order to circumvent jurisdiction. In 2012, Homeland Security seized an online gambling website—bodog.com—registered in Canada by obtaining a warrant that ordered American-based TLD operator Verisign to redirect users to a law enforcement notice (Geist, 2012). This raises questions over US jurisdictional control of the DNS as many key TLD operators are based in the United States (Kravets, 2012).

Domain name seizures also raise questions about collateral effects on the 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 because it contains a subset of infringing content. Furthermore, 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 Internet Service Provider (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. In 2011, some American legislators attempted to curb online piracy through the proposed Stop Online

Piracy Act (SOPA) and the PROTECT IP Act (PIPA). The bills would have heightened criminal penalties for piracy and enabled law enforcement to require information intermediaries to block access to infringing websites. Going much further, however, the bills would have required ISPs to locally redirect DNS lookups for sites that were believed to contain content that violated intellectual property rights.

Local redirection is often used by governments to block social media and other content. In March 2014, the Turkish government used local redirection to censor Twitter and YouTube (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 (Grossman, 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 (DeNardis, 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 article on the security concerns raised by PIPA and local redirection, Internet pioneer Steve Crocker et al. (2011) 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” (p. 2). 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 et al., 2007).

The 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 false bank login page—to collect personal or financial information from victims. They are also used by states to achieve goals such as content control. For example, the Great Firewall of China is known to use injection techniques to censor 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 sometimes 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 spurred 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 generic top-level domains (gTLDs) for brands and organizations. Beginning in 2012, 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.

Non-commercial alternate roots have also emerged, 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 arose on the Web. Calls for a decentralized and 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 is dedicated to selling illegal drugs, and that most of the traffic on the network direct 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 its citizens, as well as who and how it can be accessed. States such as North Korea (Grothaus, 2014) and Iran (Ungerleider, 2012) 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 article 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). These pressures helped motivate ICANN to proceed with internationalized domain names.

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 that 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 (Internet Architecture Board [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 in a way that is universally consistent. 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.

The Internet, as designed, requires a globally consistent name and number space, which in turn requires a universally consistent root. Without a single name and number space, the Internet would not be a universal network and instead fragment into non-interoperable segments. 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, by appending their own root zone file to IANA's root zone file (Higgs, 2001; SSAC, 2006). However, this does not guarantee that there are no overlapping name assignments across the entire constellation of alternate roots. Moreover, there are currently no other mechanisms or technical ways of ensuring the coordination of all alternate root and name system operators (SSAC, 2006).

Internet stability and freedom depend on the DNS

One significance of this article is that it dispels the narrative that the administration of the DNS is just a clerical or neutral function. 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 are not merely technical issues; how the DNS is governed is a critical public policy concern, with implications for Internet stability, security, freedom of expression, commerce, property rights, and privacy.

This article also contributes to the growing body of scholarship that establishes the sometimes concealed politics underlying technical infrastructures and how they can be co-opted for political, economic, or other goals. The rationales presented in this article for co-opting the DNS are diverse and include the following:

- 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 infrastructure as a site of global power. Other examples include three-strikes policies in which ISPs engage in a voluntary mechanism to 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.

The examples herein also suggest that the increasing DNS politicization raises troubling possibilities for destabilizing systems of Internet governance. Power struggles over DNS control and an increasing turn to the infrastructure increase the possibility of transforming the DNS from a universally consistent system to one that varies based on geography, constituency, or technology.

Concerns about fragmentation are closely related to concerns about stability and reliability. The interventions described in this article impact the stability and consistency of the DNS lookup process by changing the content and therefore quality of authoritative records, impacting the consistency of lookups historically imbued in the DNS. 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.

A third concern is security. The DNS is vulnerable to 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.

A fourth destabilizing concern relates to human rights. The DNS interventions described herein can all be used to block or censor content or otherwise limit 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, or participate in the global economy.

A final destabilizing 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.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Anishchuk A (2014) Russia eyes measures to fend off western internet threat: Kremlin. *Reuters*, 19 September. Available at: http://www.reuters.com/article/2014/09/19/us-russia-internet-idUSKBN0HE1F320140919

Bortzmeyer S (2015) IETF draft: DNS privacy considerations. Available at: https://tools.ietf.org/html/draft-ietf-dprive-problem-statement-01

Bradshaw S, DeNardis L, Hampson F, et al. (2015) The emergence of contention in global internet governance. In: *Global commission on internet governance paper series, paper no. 16*. Available at: https://www.cigionline.org/sites/default/files/no17.pdf

Braman S (2012) Privacy by design: networked computing, 1969–1979. *New Media & Society* 14(5): 798–814.

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, et al. (2011) Security and other technical concerns raised by the DNS filtering requirements in the PROTECT IP bill. Available at: http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf

Daigle L (2004) WHOIS protocol specification, RFC 3912. Available at: https://www.rfc-editor.org/info/rfc3912

Daigle L (2015) On the nature of the internet. In: *Global commission on internet governance paper series, paper no. 7*. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf

DeNardis L (2009) *Protocol Politics: The Globalization of Internet Governance*. New Haven, CT: Yale University Press.

DeNardis L (2012) Hidden levers of internet control. *Information, Communication & Society* 15(5): 720–738.

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

Diao Y and Lia M (2012) DNS extension for autonomous internet (AIP): IETF internet draft. Available at: https://tools.ietf.org/html/draft-diao-aip-dns-00

Fältström P, Hoffman P and Costello A (2003) Internationalizing domain names in applications, RFC 3490. Available at: https://www.rfc-editor.org/info/rfc3490

Geist M (2012) Bodog.com case sends warning to all Canadian websites: Geist. *The Star*, 3 March. Available at: 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.

Grossman L (2009) Iran Protests: Twitter, the Medium of Movement. *Time Magazine*, 17 June. Available at: http://content.time.com/time/world/article/0,8599,1905125,00.html

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

Hallam-Baker P (2014) Internet-draft expiring 11 May 2015 (DNS privacy and censorship: use cases and requirements).

Harlan C (2010) South Korea tries to block Twitter messages from North. *The Washington Post*, 21 August. Available at: 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*. Available at: http://www.politechbot.com/p-02077.html

IAB (2000) IAB technical comment on the unique DNS root. Available at: https://www.ietf.org/rfc/rfc2826.txt

ICANN (1999) Uniform domain name dispute resolution policy. Available at: https://www.icann.org/resources/pages/policy-2012-02-25-en

ICANN (2009) Internationalized domain names. Available at: https://www.icann.org/resources/pages/idn-2012-02-25-en

ICANN (2012) New generic top-level domains-application comment details. Available at: https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/6191

ICANN (2014) 'Motion to quash writ of attachment' in the US district court for the District of Columbia. Available at: 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*, 6 March. Available at: 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. Available at: https://www.rfc-editor.org/info/rfc4185

Kuerbis B and Mueller M (2011) Securing the root. In: DeNardis L (ed.) *Opening Standards: The Global Politics of Interoperability*. Cambridge, MA: The MIT Press, pp. 45–62.

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

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. Available at: https://censorbib.nymity.ch/pdf/Lowe2007a.pdf

Lynn S (2001) Discussion draft: a unique authoritative root for the DNS. Available at: http://archive.icann.org/en/meetings/stockholm/unique-root-draft.htm

MacKinnon R (2006) China's New Domain Names: Lost in Translation. Available at: http://www.circleid.com/posts/chinas_new_domain_names_lost_in_translation/

MacKinnon R (2012) *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

McMillan R (2010) China's great firewall spreads overseas. *Computerworld*, 25 March. Available at: http://www.computerworld.com/article/2516831/security0/china-s-great-fire-wall-spreads-overseas.html

McMillan R (2014) Verizon's perma-cookie is a privacy killing machine. *Wired*, 27 October. Available at: http://www.wired.com/2014/10/verizons-perma-cookie/

Marsan CD (2006) Native language domains threaten 'Net. *NetworkWorld*, 27 March. Available at: 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. Available at: http://www.theregister.co.uk/2009/07/28/comcast_dns_hijacker/

Miller J (2014) Iraq blocks Facebook and Twitter in bid to restrict Isis. *BBC News*, 26 June. Available at: http://www.bbc.com/news/technology-27869112

Mockapetris P (1987a) Domain names: concepts and facilities, RFC 1034. Available at: https://www.rfc-editor.org/info/rfc1034

Mockapetris P (1987b) Domain names: implementation and specification, RFC 1035. Available at: https://www.rfc-editor.org/info/rfc1035

Mueller M (2001) Competing DNS Roots: creative destruction or just plain destruction? Available at: http://arxiv.org/ftp/cs/papers/0109/0109021.pdf

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

Mueller M and Van Eeten MJG (2013) Where is the governance in internet governance? *New Media & Society* 15(5): 720–736.

Musiani F (2012) A decentralized domain name system? User-controlled infrastructure as alternative internet governance. Available at: http://web.mit.edu/comm-forum/mit8/papers/Musiani_DecentralizedDNS_MiT8Paper.pdf

NTIA (2014) *Keynote Address by Lawrence E. Strickling Assistant Secretary of Commerce for Communications and Information 'Who Governs the Internet? A Conversation on Securing the Multistakeholder Process'*. Washington, DC. Available at: https://www.ntia.doc.gov/speechtestimony/2014/keynote-address-assistant-secretary-strickling-american-enterprise-institute

Plante NA (2004) Practical domain name system security: a survey of common hazards and preventative measures. Available at: http://www.infosecwriters.com/text_resources/pdf/dns-security-survey.pdf

SSAC (2006) Alternative TLD name systems and roots: conflict, control and consequences. Available at: 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. Available at: https://www.icann.org/en/system/files/files/sac-056-en.pdf

Seltzer W (2011) Exposing the flaws of censorship by domain name. *IEEE Security & Privacy*. Available at: http://wendy.seltzer.is/writing/COICA-IEEE.pdf

Siegler MG (2011) Twitter confirms that they're being blocked in Egypt. *TechCrunch*, 25 January. Available at: 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*, 25 February. Available at: http://www.wired.com/2008/02/pakistans-accid/

Tuysuz G and Watson I (2014) Turkey blocks YouTube days after Twitter crackdown. *CNN*, 27 March. Available at: 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. Available at: http://www.fastcompany.com/1819375/irans-second-internet-rivals-censorship-chinas-great-firewall

Vargas Leon P and Kuehn A (2015) The Battle for Critical Interner Resources: South Amerca vs. Amazon.com, Inc. *The Law, State and Telecommunications Review, Brazilia* 7(1) p37-58.

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

Weber R (2009) *Shaping Internet Governance: Regulatory Challenges*. London; New York: 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*. Available at: 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, CT: Yale University Press.

Author biographies

Samantha Bradshaw is a research associate at the Centre for International Governance Innovation (CIGI) in Waterloo, Canada. She contributes to CIGI's work on Internet governance and is a key member of a small team facilitating the Global Commission on Internet Governance. Samantha holds a joint Honours BA in Political Science and Legal Studies from the University of Waterloo, an MA in Global Governance from the Balsillie School of International Affairs and will be pursuing her D.Phil in Information, Communication and the Social Sciences at the Oxford Internet Institute.

Laura DeNardis is a professor in the School of Communication at American University in Washington, District of Columbia (DC). She is the author of *The Global War for Internet Governanc*e (Yale University Press 2014) and other books and serves as the Director of Research for the Global Commission on Internet Governance. She holds Bachelor's and Master's degrees in Engineering from Dartmouth College and Cornell University, a PhD in Science and Technology Studies from Virginia Tech, and completed a Postdoctoral Fellowship at Yale Law School.