Communications of the Association for Information Systems

Volume 30 | Number 1 Article 21

5-1-2012

The Domain Name System—Past, Present, and Future

Michael Brian Pope
Department of Management & Information Systems, Mississippi State University, mpope5678@gmail.com

Merrill Warkentin
Department of Management & Information Systems, Mississippi State University

Leigh A. Mutchler
Department of Management & Information Systems, Mississippi State University

Xin (Robert) Luo
Anderson School of Management, University of New Mexico

Recommended Citation
Pope, Michael Brian; Warkentin, Merrill; Mutchler, Leigh A.; and Luo, Xin (Robert) (2012) "The Domain Name System—Past, Present, and Future," *Communications of the Association for Information Systems*: Vol. 30, Article 21.
Available at: http://aisel.aisnet.org/cais/vol30/iss1/21

This material is brought to you by the Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Communications of the Association for Information Systems

CAIS

The Domain Name System—Past, Present, and Future

Michael Brian Pope

Department of Management & Information Systems, Mississippi State University

mpope5678@gmail.com

Merrill Warkentin

Department of Management & Information Systems, Mississippi State University

Leigh A. Mutchler

Department of Management & Information Systems, Mississippi State University

Xin (Robert) Luo

Anderson School of Management, University of New Mexico

Abstract:

The Domain Name System (DNS) is a critical component of the global Internet infrastructure. Throughout its history, its design and administration has experienced significant dynamic changes as the Internet itself has evolved. The history of the DNS is divided into six eras, based on underlying technological and administrative themes within each era. Developments in its governance, its application, and in other factors are discussed. Future directions for DNS use and abuse are explored, along with challenges in its future governance. Finally, a proposed research model is included to guide future study of the DNS evolution and its influences from political, legal, psychological, sociological, and technological perspectives.

Keywords: Domain Name System (DNS), Internet architecture, historical perspective, forecast, politics, IPv4, IPv6, Internet governance

Volume 30, Article 21, pp. 329-346, May 2012

The manuscript was received 6/23/2011 and was with the authors 1 week for 1 revision.

IPR2025-01400
CrowdStrike EX1021 Page 2

I. INTRODUCTION

As a critical component of the Internet's infrastructure, the Domain Name System (DNS) is the translation system that turns an Internet host name (domain name) into the unique series of numbers which constitute an Internet Protocol (IP) address for each specific domain name. Similar to a telephone number, an IP address is required to route packets and coordination signals throughout the Internet system. A simple yet sophisticated system, the DNS handles up to 20 billion address translation or "look-up" requests per day [Hogge, 2008]. Every time someone wishes to access a website, whether the request is handled by one of the thirteen core servers known as the *"root" servers,* or a server lower on the Internet hierarchy that takes the bulk of the requests, the DNS is the key to correct completion of that request.

Since its creation in the 1980s, the DNS has successfully served the needs of Internet users. It has experienced its share of issues, including those concerning its maintenance organization, technical and security troubles, structural concerns, and disagreements over how it should be governed. These issues, as well as others yet to be seen in the future will certainly impact the continued use of the DNS and the associated networks. As prior studies have attempted to investigate the DNS's technological properties, this article presents a more comprehensive analysis of various DNS characteristics. In essence, it begins by revisiting DNS development, breaking its history into six "eras"—which we believe are the Digital Era, Development Era, Domain Name Era, Dot-Com Era, Dot-Crunch Era, and the Decay Era. Furthermore, we explore some of the many managerial and technological issues affecting the DNS in 2011. We conclude our discussion by offering an educated forecast as to the future of the DNS, and a proposed model to serve as a guide for researchers to continue the exploration of the DNS and its many influences from many perspectives, such as political, legal, sociological, psychological, and technological change, giving context to the process of its prior development.

II. THE DNS PAST

In order to see where we are going, it is often helpful to consider where we have been. In light of that, a brief overview of the history of the DNS is warranted before we discuss the present or the future.

The Digital Era

In 1969, one of the first wide area networks (WAN) began to operate [Guice, 1998; Rogers, 1998]. This network was dubbed ARPANET after the funding organization, The U.S. Department of Defense Advanced Research Projects Agency (ARPA). The system that administered the translations of names to addresses for each ARPANET host computer at that time was called HOSTS.TXT, named after the core data file in the system. At first only four nodes connected by 50kbps lines spanned the west to east coasts of the United States, but by 1971 a total of fifteen nodes with twenty-three hosts linked major universities across the country. Updates to the HOSTS.TXT system were performed by e-mail change requests and FTP transfers. These updates were constantly required in order to avoid confusing the network with out-of-date versions. Although inconvenient, this allowed a primitive form of name-based references to be used over ARPANET [Sun, 2009].

The Development Era

In 1972, shortly after the development of the Ethernet network protocol by Bob Metcalfe and his colleagues at Xerox PARC, the ARPANET expanded internationally by adding nodes in England and Norway and bringing the node total to twenty-nine [Harvard University, 2000]. A connection problem made by the lack of protocol standardization was being tackled by the International Network Working Group (INWG), leading the way for systems such as Telnet and Datapac, and creating the Internet we know today [Cerf, 1995; Edmondson-Yurkanan, 2007].

ARPANET continued to grow, and by 1975 a total of sixty-one nodes were in existence. Separate networks with connections to ARPANET began to spring up, including NASA's SPAN, BITNET at the City University of New York, and CSNET. The latter was the result of collaboration between the University of Delaware, Purdue University, the University of Wisconsin, RAND Corporation, and Bolt Beranek and Newman (BBN), funded by the National Science Foundation (NSF). The goal of CSNET was to connect computer science departments at institutions that were without ARPANET access. By 1983, the node count totaled 113 and security concerns resulted in the ARPANET being split into the MILNET network for military sites with sixty-eight nodes, leaving the remaining nodes of ARPANET to be used by the computer research community [Harvard University, 2000; NSF, 2009; Sun, 2009].

IPR2025-01400
CrowdStrike EX1021 Page 3

The NSFNET, a backbone network built in 1985 by the NSF originally to connect five NSF-supported supercomputers, created such demand that it needed a major upgrade in 1988, plus plans in 1989 to move from a T1 to a T3 connection [NSF, 2009]. An explosion of connections from non-computer science researchers at universities and other organizations followed when the NSF agreed to allow self-organized networks connection to NSFNET. By 1989, ARPANET no longer existed [Harvard University, 2000].

The Domain Name Era

When ARPANET moved to the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols in 1983 [Harvard University, 2000] and became known as the Internet, the population of networks exploded. The centrally maintained HOSTS.TXT file became plagued with problems, such as traffic and load, name collisions, and consistency anomalies. It was clear that HOSTS.TXT no longer met the needs of the rapidly expanding Internet, and that a more robust system was needed. A group composed of Jon Postel, Paul Mockapetris, Craig Partridge, and others [Harvard University, 2000] met the need when they published RFC 882 in 1984 which resulted in the creation of the distributed naming system known as the DNS.

The DNS is a distributed database that allows local administration of the segments on the overall database. Data in each segment of the database are available across the entire network through a client-server scheme consisting of name servers and resolvers [Mockapetris and Dunlap, 1995]. Just as each telephone number is a unique sequence of numbers, so is the IP address for each computer on the Internet. Rather than memorizing 192.0.34.65, we can simply enter www.icann.org and the DNS translates, or resolves, the domain name to the IP address [InterNIC, 2002a].

The Dot-Com Era

Throughout the mid-90s, access to the Internet had been text-based and relatively cumbersome, assuring its use to remain with the academic and technical populations. The potential of the Internet as a medium for information sharing had just begun to be explored in full. In 1989, Tim Berners-Lee, working for CERN, proposed a new system for linking together information using hypertext [Berners-Lee, 1996]. The concept of “hypertext”—a form of document that links together other documents—was not a new one. First traced back to a paper written by Vannevar Bush in 1945, it had been addressed by other scholars and engineers such as Douglas Englebart and Ted Nelson in the 1960s. However, it was Berners-Lee who proposed the well-known standard for hypertext on the modern Internet. One further component, an easy-to-use interface, was needed for the World Wide Web to become the successful phenomenon it is today, and it did not take long for an interface to be created. In 1993, Jon Mittelhauser and Marc Andreessen were among a group of students at the University of Illinois who recognized this need and created Mosaic, the first modern Web browser [Borland et al., 2003; Yamamoto, 2003]. In 1994, Marc Andreessen joined with Jim Clark to form Netscape and release the Netscape Navigator browser, which was followed in 1995 by Microsoft’s Internet Explorer browser [Borland, 2003]. Expansion of the Internet was inevitable with the graphic-based browsers empowering virtually anyone to experience it, making a properly and reliably functioning DNS more critical than ever.

As Internet connections continued to explode, it became clear that an administering body was needed, and, in 1993, InterNIC was created by the NSF to provide Internet directory and database services, registration services, and information services [Adler et al. 1994]. Of the three participants—AT&T, General Atomics, and Network Solutions, Inc. (NSI)—NSI was by far the most important to the DNS administration of the era, providing registration services for domain names. As such, it was particularly influential in establishing the Internet during this critical period of growth and formation, becoming, for a time, synonymous with domain registration.

The DNS uses a tree directory structure with the right-most portion of each domain name made of three letters and being the base, or root, of the directory structure, called the top level domain (TLD). The first TLD names included the following seven familiar extensions; .com, .edu, .gov, .int, .mil, .net, and .org. Besides the three-letter TLDs, over 250 two-letter TLDs were established for countries and territories, and a single unique TLD, .arpa, was established for administrative purposes [ICANN, 2008b]. As use of the Internet increased, so did domain name registrations. Between 1993 and 1996, registrations of the TLDs .com, .net, and .org rose from an average of 400 per month to 70,000 per month [Mueller, 1997]. While the number of possible character iterations for a domain name is limitless, the number of sensible and useful names is actually quite limited. Fueled by the realization of this limitation, in 2000, new TLD additions were discussed and between 2001 and 2003, a total of thirteen new general and special-use TLDs were introduced. The new general TLDs were .biz, .info, .name, and .pro. The new special-use TLDs were .aero, .coop, .museum, .asia, .cat, .jobs, .mobi, .tel, and .travel [ICANN, 2008b].

IPR2025-01400
CrowdStrike EX1021 Page 4

The Dot-Crunch Era

Through 1995, the NSF had subsidized the domain name registration costs, but with Internet use becoming mainstream and commercialized, and with the number of registrations skyrocketing, the NSF implemented a registration fee of $50 to begin on September 14, 1995 [NSF, 1995]. This new cost slowed down what had become a domain name grabbing free-for-all by some speculators, known as *cybersquatters,* who registered domain names with the hopes of making a profit by selling the name. Speculation was curbed, but not completely stopped, as some names had and were expected to be worth well over the new $50 registration fee. In fact, examples of a few of the outrageous amounts domain names sold include business.com for $7.5 million, loans.com for $3 million, autos.com for $2.2 million, and savings.com for $1.9 million [DomainNameStuffetc.com, 2002].

Two of the more famous cybersquatter cases include that of toysrus.com and mtv.com. By the time each of these well-established companies realized the future impact of the Internet and the associated requirement to own their respective company name domains, they each found themselves unable to obtain them. In the case of Toys R Us, a young boy who saw the opportunity for free toys and bikes purchased toysrus.com. With MTV, it was a VJ seeking leverage in an upcoming contract negotiation who predicted mtv.com would be his job security guarantee [Warkentin, 1999].

The Internet, which had started as a network for scientific and military purposes, rapidly became an integral part of everyday life for many organizations and people around the world. As an unregulated form of communication, majority acceptance of the policies required administrative governance by an unbiased organization. In 1998, the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit Department of Commerce contractor [Fuller, 2001] was formed to fill that need. Besides overseeing the security, stability, and interoperability of the Internet, ICANN's duties included two that were DNS specific; the coordination of allocations and assignments of the DNS and the coordination of the operation and evolution of the DNS system [ICANN, 2008c].

Ownership of domain names continued to be a frequent problem, along with complaints about the process of domain name sales, the majority of which were being handled by Network Solutions, Inc. (NSI). ICANN hoped to improve the resolution of both of these issues by allowing more competition and by establishing mandatory arbitration of trademark claims. Competition was established by allowing America Online and register.com, among others, to join in the sale of domain names. Ownership disputes related to gTLD or certain country-code TLDs (ccTLD) where claims of trademark or service mark infringements existed, or where accusations of abusive domain name purchase intent were present, would be resolved through an arbitration process. Beginning in late 1999, in order to be allowed to process a purchase, purchasers would be required to agree to the Uniform domain name Dispute Resolution Policy (UDRP) [Diéguez, 2008; Elias and Stim, 2007; InterNIC, 2002b]. The UDRP process includes five steps, beginning with the accuser filing a complaint and followed by the accused party filing a response. Next, a panel selected by the dispute resolution service provider reviews the complaint and makes a decision. Once decided, all parties are notified, and finally the change to the domain name ownership is implemented [WIPO, n.d.].

The Decay Era

The last DNS "era" and the one in which we now reside we call the Decay Era. The DNS has remained the accepted system for the Internet, but problems have occurred, and more are expected; some are due to flaws known since the beginning, and some are due to flaws like the "Kaminsky bug" discovered in 2008 [Prince, 2008; Wattanajantra, 2008]. DNS is further challenged by the progressive push to change the Internet from the traditional Internet Protocol version 4 (IPv4) to the sixth version (IPv6) to solve a myriad of technical problems with the original implementation, not the least of which is the theoretical maximum number of addresses available within the protocol [Lee et al., 1998]. While most major DNS server programs have been updated to support the necessary changes, such a fundamental shift in the infrastructure of the Internet makes it a ripe time for advocates of particular technologies that might replace DNS to push for the implementation and proliferation of such protocols. DNS will have to adapt to these changes and may find itself facing increasing competition—factors such as politics [Greenemeier, 2011; Kravets, 2011] and technological availability [Greere, 2010] may make a replacement viable.

III. THE DNS PRESENT

Although indisputably the worldwide standard at present, the domain name system does not find itself facing a lack of challenges in the immediate future. We continue, therefore, with an outline of some of the more serious challenges.

Organizational

The ICANN domain name system is the most prevalent one, but its dominance is not absolute; there are several smaller systems available using the same protocols. OpenNIC [OpenNIC, 2009], UnifiedRoot [UnifiedRoot, 2009],

IPR2025-01400
CrowdStrike EX1021 Page 5

and Public-Root [Public-Root, 2009] are but three alternative registrars for Internet domain names. Although all three of these are miniscule compared to ICANN's mainstream offerings, it does not take much imagination to see that, given the political unrest seen in the early 2000s, as well as in the name of general independence, a number of larger organizations, including the Chinese government or Russian government, may wish to begin their own registry to keep tighter control on the Internet use of their citizens, both in terms of communication and as commercial interests. It is possible that these could run alongside the ICANN system somehow, through various means such as Web portals or automated software reconfiguration, but it is likely that these would be too cumbersome for most users to bother with—and legislation may even require the use of a government-approved registry system.

Technical

A number of technical issues must be addressed for the domain name system to continue as the standard in the future. Not the least of these is the change of the Internet Protocol IPv4 to IPv6. IPv4, the predominant version as of 2011, is ubiquitous on networking equipment throughout the world, which is, ironically, part of the problem. Due to the 32-bit length of IPv4 addresses, there are nearly 2^{32}, or approximately 4 billion, addresses possible. The Internet Engineering Task Force (IETF) is an international organization, chartered by the Internet Society (ISOC), and comprised of voluntary Internet professionals whose mission is to "make the Internet better" [IETF, 2009]. The Internet Assigned Numbers Authority (IANA), chartered by the ISOC and run by ICANN, is the IP address allocation agency as of 2011. After allocating an IP address to a Regional Internet Registry (RIR), the IANA reports the assignment to the IETF [IANA, 2009]. IP address networks are divided into five different classes [Held, 2002]. There can be sixty-four class "A" networks, with each of these holding onto over 16 million addresses, most of which are unused. Similar problems occur with class "B" networks. This has made most networks, with a tiny allocation of 256 addresses per network, comprise the vast majority of Internet address allocations to date. Class "D," reserved for multicast, and class "E," reserved for experimental allocations, are both considered unsuitable for general use, which leaves a rapidly dwindling number of addresses, necessitating the shift to the newer 128-bit IPv6, which can support up to 2^{128} addresses [IANA, 2009], or more than $7.9 * 10^{28}$ times the number of addresses available with IPv4.

Adoption of the IPv6 protocol is occurring most rapidly in Asian countries, particularly in Japan and China. European countries are moving more slowly but continue to steadily move to the new standard, fueled by a mandate of the European Union Commission. The United States, however, continues to move more slowly than the rest of the world in adoption of IPv6, proposed by some to be the result of a struggle among issues such as maintaining its historical powerbase over the IPv4 Internet, justifying the costs of upgrading, and the gamble of becoming incompatible with the rest of the world [Hovav and Schuff, 2005]. The DNS system with the IPv6 protocol will be able to handle new aspects of the network, but are confounded by the numerous issues of adopting IPv6 in the first place, including speculation that the transition may not actually happen at all. A more thorough discussion of these issues is beyond the scope of this article, but that does not downplay their importance to the DNS. In short, the DNS faces a major overhaul and update, while needing to retain some degree of backwards-compatibility during the long and painful transition to IPv6, if it actually succeeds.

Integrity

Security problems are an extreme concern for the DNS, because it is the first (and often the only) line of defense ensuring unsuspecting Internet users are not fraudulently redirected to websites masquerading as other popular websites, or otherwise stealing traffic that is not rightfully theirs. A number of DNS attack techniques have been identified, which grow increasingly sophisticated over time [Carli, 2003]. These include DNS cache poisoning, which involves fraudulent information in a legitimate DNS server's cache; DNS spoofing or pharming, where an adversary redirects DNS queries from a legitimate server to an illegitimate or compromised server [Bose and Leung, 2007]; and DNS ID hacking, a key technique needed to permit other attacks. Solutions to these problems are limited. However; due to the necessity of maintaining backwards compatibility, design flaws will remain. Given the bugs discovered in 2008 which cut across numerous software packages requiring many software vendors to release simultaneous releases to repair a fault [US-CERT, 2008], it is a distinct possibility that many more bugs of this nature may exist, possibly even more serious than those already encountered. This casts doubts on the reliability of the DNS standard in terms of the ability to continue serving the Internet community in a secure manner. Researchers such as Dan Kaminsky have made many other flaws with the system public, further increasing scrutiny on its efficacy in an era of heightened security concerns [Kaminsky, 2008]. In fact, Paul Mockapetris, creator of DNS, has gone on record to state that more security needs to be added, citing regrets that the original implementation overlooked such concerns and praising attempts to make it more secure, such as DNS Security Extensions (DNSSEC) [Espiner, 2008].

First formally discussed in 1993, the purpose of using DNSSEC is to add a layer of security to the DNS with public key encryption and digital signatures. In the case of receiving an e-mail, use of DNSSEC provides a method to verify that the domain the e-mail indicates it is from is actually where it is from, potentially reducing the amount of spam e-

IPR2025-01400
CrowdStrike EX1021 Page 6

mail transmissions. When an individual accesses a website, use of DNSSEC helps to ensure that the domain of the website is truly the domain the individual intends to access thereby reducing potential phishing threats. Since DNSSEC was not part of the original DNS, global use would have required voluntary adoption by DNS Server owners and solution providers. Adoption did not occur due to various implementation issues including the knowledge that DNSSEC was not a perfect solution. By the late 1990s, rather than waiting for a perfect DNSSEC, the development of alternate hardware- and software-based security systems and solutions occurred [Berlind, 2003]. As of July 15, 2010, however, the thirteen Internet root servers began to support DNSSEC, and by March of 2011, DNSSEC had been implemented in 20 percent of the TLDs around the globe [Mohan, 2011; Vaughan-Nichols, 2010].

Different language alphabets frequently contain letters that are visually the same as those in other alphabets. A homograph is a form of misspelling that uses non-Latin characters that are visually the same as a Latin character. Use of non-Latin characters that are visually the same as Latin characters in a domain name introduces a new form of phishing security issue known as *homograph phishing attacks* [Gabrilovich and Gontmakher, 2002]. Luckily, as domain names with non-Latin characters became available in the late 2000s, no noticeable trends were identified toward this form of phishing [Aaron and Rasmussen, 2010]. Some of the reasons are speculated to be that the possibility of this form of phishing was not overlooked by ICANN and Internet browser programmers and, therefore, safeguards have been set in place [Johanson, 2005; Neylon, 2010], and that professional phishers don't need to use this method to fool potential victims since they are having enough success without it [Aaron and Rasmussen, 2010].

A problem some may find not quite as severe, but a serious problem nonetheless, is the integrity of lower-level registrars. Reports have been made of these organizations behaving improperly and exhibiting a lack of good faith in their access to the namespace in what has become known as *domain tasting* [Healey, 2007]. The namespace is the total of valid domain names possible, such as yahoo.com, google.com, or thisdoesnotexist.com. A domain is "tasted" by registering the domain name and then tested to see how much traffic it received [Fulton, 2008]. If the name attracted the desired amount of traffic, the domain was retained. If, however, the domain name did not perform as hoped, the name was returned, and the registration fee was refunded as allowed by the Add Grace Period (AGP) rule provided by ICANN. This resulted in 32.7 million out of 35 million—more than 93 percent—of registrations being refunded in April of 2006 alone [Parsons, 2006]. Such gross abuse has led to policy changes which have significantly curtailed this practice [ICANN, 2009].

Unfortunately, there are still more issues that call into question the integrity of at least some lower-level registrars [Alexander, 2006]. Through what is known as *domain pinching,* domain names that a registrar believes are likely to be highly popular are claimed for themselves and later auctioned off to the highest bidder. Another form of inappropriate behavior called *domain stuffing* is the all-too-often-seen practice of pointing a domain name to a generic index page that may include targeted ads or pay-per-click links. This form of misdirection may succeed by using a domain name that is similar to or a common misspelling of an existing legitimate domain name.

Structural

DNS is highly prolific and most exchanges on the Internet involve DNS at least at some level. However, many critics have leveled considerable negative assessment to the DNS system as it exists in 2011, which is arguably not well designed for the purpose that it serves. Problems include security, vulnerability, political aspects, [Ramasubramanian and Sirer, 2004] intellectual property, and the concerns of private individuals [Foner, 2001]. Some, in fact, call for the outright replacement of DNS, despite the difficulties it may present [Foner, 2001]. However, it is likely that the DNS is too deeply intertwined with network software to be completely replaced at the interface level [Deegan, Crowcoft, and Warfield, 2005]. Nevertheless, major structural changes can be affected that would have negligible impact on client applications in terms of functionality or code changes.

These charges are not inaccurate. The DNS system is not perfect. Many efforts have been undertaken to attempt to overcome its shortcomings, including attempts at altering its structure. Peer-to-peer technology is one likely candidate for this, due to its resiliency against denial-of-service attacks, high-level scalability, and load balance assistance in handling the network demands that DNS faces; as such, systems such as the Cooperative Domain Name System (CoDoNS) have been proposed to attempt to leverage the benefits of peer-to-peer strategies [Ramasubramanian and Sirer, 2004]. The introduction of more secure protocols such as DNSSEC may make it more practical to execute such changes, which we may see now that DNSSEC is supported on the thirteen root servers and support is rapidly spreading on others, [Mohan, 2011; Vaughan-Nichols, 2010]. On the other end of the spectrum, some propose reengineering the DNS from its distributed system to a centralized overall system for performance purposes [Deegan, Crowcoft, and Warfield, 2005]. As such, the very physical structure of the DNS is not a static entity; rather, it is in flux and may considerably develop, or may eventually even be totally replaced.

IPR2025-01400
CrowdStrike EX1021 Page 7

Political

As mentioned previously, the possibility exists that other countries or organizations may start their own domain name registries for their own purposes. This is not the limit for potential political interference in domain name registration. Moves to censor the Internet in western countries such as Italy [Warner, 2007], Australia [Bryant, 2008], and the United States [Bambauer, 2011] join other well-known censorship initiatives in other countries such as China [Zittrain and Edelman, 2003]. That the governments of these influential countries seem to be pushing for such movements in their own sphere of influence makes it quite possible that they may move their interests abroad and attempt to exert pressure on ICANN to modify their policy to better fit their demands. ICANN is under the employ of the U.S. Department of Commerce as a contractor and is a private organization with nonprofit status dedicated to maintaining the coordination of aspects of the Internet such as the DNS [Fuller, 2001; ICANN, 2007]. These services are vital, but ultimately ICANN's authority is derived by the mutual consent of the Internet community. That authority theoretically could be revoked at any time, and in many cases it would take only a relatively limited amount of legislation to entirely deprive ICANN of power in a country, and possibly many countries. In order to prevent the emergence of alternative domain registrars backed by the resources of a large country, ICANN may need to at least partially acquiesce to such interests.

Governance

As with all sizable organizations, there have always been those who have disagreed with their decisions, and ICANN is no exception. In this vein, decisions to modify the DNS hierarchy caused considerable controversy (see Figure 1 for the DNS Hierarchy). In particular, significant changes to the way that TLDs are handled have occurred. ICANN has historically been well-known for tightly regulating the TLDs with their addition or subtraction being cause for considerable publicity. However, the process to allow the public to purchase top-level domains for the first time was finalized in June of 2011, albeit accompanied by a hefty $185,000 price tag, no guarantee of approval, and limited to a three-month application window [Rashid, 2011; Shankland, 2011]. This raises a number of issues with censorship being among them. The .xxx TLD has often been proposed for pornography-related websites, raising issues about ICANN entering the content–compliance business, was initially rejected [ICANN, 2006], only to be reconsidered in June of 2010. ICANN determined the application should be reconsidered since the last application rejection in 2007 was cited as going against the policy to be neutral, objective, and fair. At that time, one registrar estimated a $30 million/year revenue stream would result from the sale of .xxx domain names [White, 2010]. To the confusion of and disapproval by family, religious, free speech, and adult entertainment groups, ICANN approved the addition of the .xxx TLD in March of 2011 [Blue, 2011; Cheng, 2011]. The registrar ICM Registry, considered to be the driving force behind the push for the TLD approval, has already presold more than 250,000 domain names equating to roughly $20 million, and are projecting annual sales of about $200 million for domain names under the new porn TLD [Blue, 2011]. ICM Registry not only submitted an application for the unsponsored gTLD .xxx, but for a .kids gTLD as well [ICANN, 2000] under the auspices that if the application is accepted, such gTLDs may further provide separation of content-specific sites and ideally provide simpler methods to prevent the unintended access of sites with inappropriate content for children. The controversy continues, however, as the majority of the .xxx presales are believed to have been made not for the expected use, but for the purpose of preventing the domain name use [Blue, 2011].

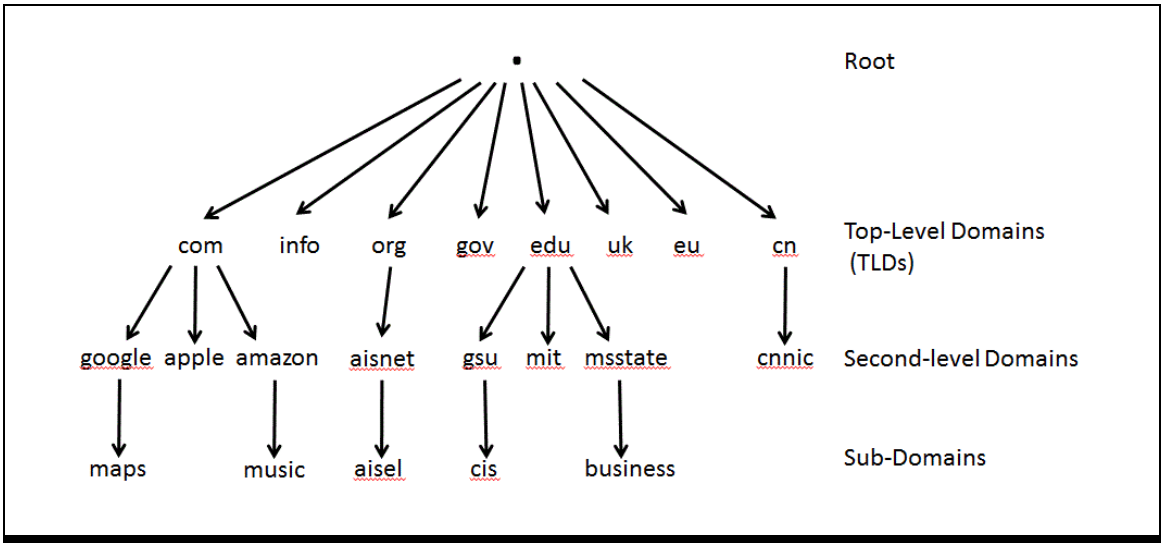

Figure 1. Illustration of DNS Hierarchical Structure

IPR2025-01400
CrowdStrike EX1021 Page 8

Another example, quality control, was once very tightly regulated with care being taken to ensure that the domain names assigned to TLDs complied with the guidelines keeping the categories meaningful [Postel and Reynolds, 1984]. Some TLDs are tightly regulated, such as those under .edu [EDUCAUSE, 2009]. On the other hand, others, such as .com, have little to no regulation, in part due to the fact that one can purchase a domain name under some TLDs in seconds, precluding much, if any, human involvement. As an example, consider a proposed geographically-oriented TLD such as .paris which would be a TLD for websites related to Paris, France. A lack of domain name regulations opens up the possibility for a domain name like ihate.paris, a website unlikely to be positively focused on Paris, France, and raising the larger question of who determines the criteria for admission. Trademark issues may also become a factor, as these new TLDs could end up contested in court on trademark and other issues, as other domain names are. Of greater concern, however, is the proposal that new TLDs can have non-Roman characters within them [ICANN, 2008a]. On the surface this may not seem to be a problem; however, Roman characters are the standard for keyboards throughout the world, and users would have to exert considerable effort to enter characters in a language other than their own. This could be used as a mechanism for limiting effective access to some websites from the outside world.

The Business of the DNS

As the Internet develops into multiple knowledge repositories, social networks, e-businesses, virtual educational institutions and a myriad of other tools for personal, business, and educational use, DNS issues must be contended with, for example, those related to the global expansion of the Internet as illustrated by the global IP address distribution shown in Figure 2, as well as the numerous new issues that continue to surface. As the Internet expands, becoming integrated into our daily lives and increasingly more critical to the livelihood of organizations and individuals, so it becomes not only a tool or a resource but a business in itself. As a result, networks are becoming increasingly complex, requiring the multiple IP resources being used by organizations to be managed. This critical need is being met by tools such as IP address management (IPAM) software [Garrison, 2011], and by registrars like Oversee.net providing services beyond the simple purchase of a domain name [Oversee.net, 2010]. For example, Oversee.net offers brokerage services for the buying and selling of domain names, comparing their service to that of the brick-and-mortar real estate brokering that has been taking place for centuries. Much like a sophisticated advertising firm, Oversee.net also assists with attracting customers to websites through their "monetizing direct navigation traffic" services. Even those who wish to build their e-business on the Internet itself can do so with Oversee.net's Emerging Business Division.

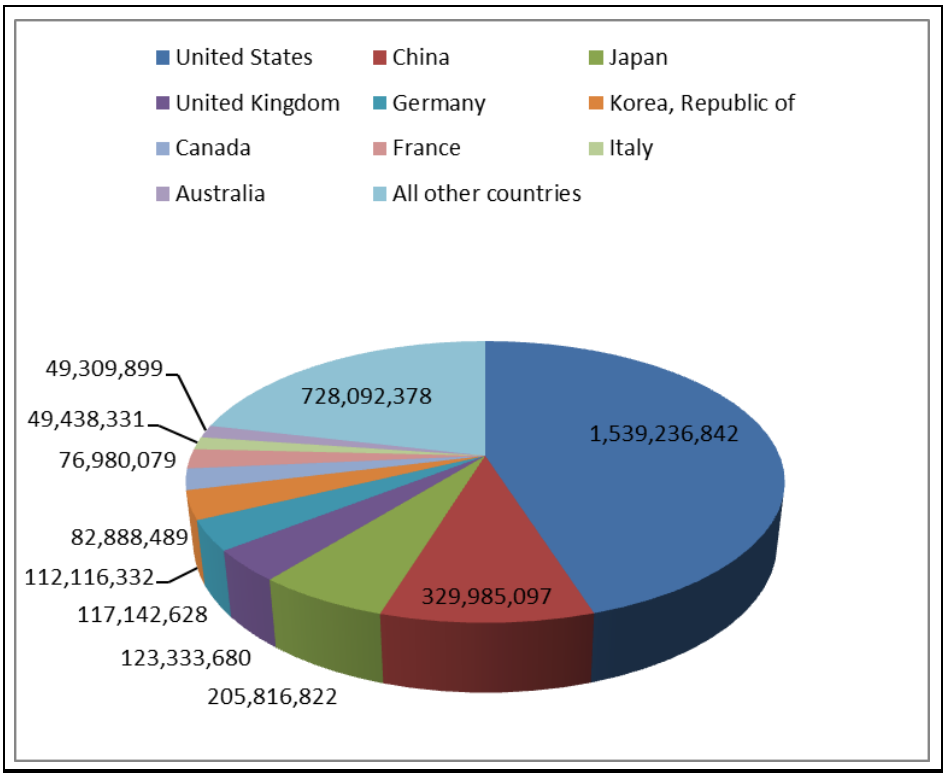

Figure 2. Global IP Address Distribution by Country [MaxMind, 2011]

IPR2025-01400
CrowdStrike EX1021 Page 9

IV. THE DNS FUTURE

To presume to be able to predict the future with great accuracy, particularly in a realm so rapidly changing as technology, especially when it is so deeply intertwined with many other dynamic factors from across the modern world structure, may seem a bit presumptuous. We must recognize the limitations of trying to predict the future in a realm that changes so rapidly, and with so many technological, political, and economic influences. Nevertheless, based on an objective assessment of these trends and using a reasonable extrapolation to guide our analysis, we offer forecasts for the answers the DNS and ICANN may present for the challenges facing it in the decade of the 2010s.

Use of Extended Characters in TLDs

Chinese Characters

As a step toward a globally compatible Internet, in June of 2010 ICANN approved Chinese language TLDs, an approval preceded by approvals for Egypt, Russia, Saudi Arabia, and the United Arab Emirates IDNs in April of the same year. This change to allow new internationalized domain names (IDNs) to now be registered using non-Latin characters, such as Arabic, Cyrillic, or Chinese, that are local to a specific country opens up Internet use to large groups of individuals in the world who have so far been unable to access the Internet due to this language barrier [Abolins, 2010; Sayer, 2010].

Latin Characters

Use of non-Latin characters requires solutions to technological hurdles, with the Internet Engineering Task Force providing the base technology solutions. The IDNs will begin with the characters xn with a series of letters and numbers to represent the non-Latin characters, translated by the users' browser into the international characters [Sayer, 2010]. Input of the non-Latin characters from a user's keyboard in order to access the website or to use network tools such as nslookup or WHOIS, however, will require a keyboard or other input device capable of entering the special characters [Abolins, 2010]. This difficulty may play a large part in whether the IDNs will be used very much beyond China and other cultures that tend to be more insular. The driving force behind this will likely be commerce, as well as a desire to communicate with one another; furthermore, the use of standard TLDs is something that Internet users overwhelmingly prefer. Many subtle technical challenges also come with the change to Unicode [Abolins, 2010]. Many network tools which are considered ubiquitous to administrators were originally written long before Unicode was even considered as a possible element in DNS records, instead using ASCII, which relies on single-byte character codes. Fortunately, solutions exist, such as converting Unicode records into ASCII-compliant strings known as *Punycode* with the aid of various utilities and using these Punycode strings in lieu of the real domain name. Nevertheless, this is an awkward solution, and proper Unicode support will require modification of the software, which may prove extensive in more sophisticated programs.

Unicode

Problems with authentication are also found with the Unicode transition [Abolins, 2010]. WHOIS, the standard for identifying who is responsible for a DNS record, has difficulty with these strings. Although alternatives exist, such as using Punycode with more cooperative utilities and then doing a reverse lookup using the IP address, these are awkward and are likely to cause problems for applications that may rely on more traditional WHOIS commands and interfaces.

The problems in the Unicode arena span from annoyances to severe potential threats with the prospect of homographic attacks [Abolins, 2010]. These attacks use the extensive library of characters available to Unicode to find specific characters that look identical to legitimate characters. Thus, you might attempt to log in to your mail account at mail.yahoo.com by clicking a link. It would look the same to the human eye, and the URL would look legitimate. Unfortunately, one of those characters could be altered to look like the original, sending you to a completely different site—possibly a fraudulent one, which may attempt to intercept passwords or accomplish other damage. Although removing offending sites from the records, once found, would be simple, a question arises in terms of how long a hypothetical site could get away with it. Furthermore, simply disabling such a site is cold comfort for anyone who has had their e-mail compromised by individuals with unknown intent on another continent. While homographic attacks are mostly hypothetical at this time, it is hardly difficult to imagine phishers and others beginning to use this potential security hole in earnest in the near future.

New TLDs Will Become a Norm

Significant changes were made in the ICANN handling of TLDs in 2010 and 2011, ultimately leading to the viability of purchasing new TLDs for use by private entities [Shankland, 2011]. The new generic TLDs (or gTLDs) will enable addresses to end in almost any word in any language, thereby enabling stronger and more creative brand

IPR2025-01400
CrowdStrike EX1021 Page 10

identification [ICANN, 2011]. This may lead to a new round of domain name and trademark disputes, historically a source of considerable legal activity [Davis and Warkentin, 2001], and may be even more heated, as a custom TLD is more difficult to replace than a regular domain name with a generic TLD. Existing TLDs will still see much contention for domain names—many companies will want to be available at a more "traditional" address, at least for a long while, so Google may be reachable with main.google and google.com simultaneously. This may eventually also result in ICANN being forced to judge content even more than before to determine how to handle TLD management.

Uneventful IPv6 DNS Conversion

This will be relatively painless, as many, if not most, major DNS software packages support the IPv6 version alongside IPv4. As such, any well-maintained site with updated software may very well need only some slight reconfiguration to provide full IPv6 functionality. A far more pressing concern is in the actual deployment of IPv6; in short, DNS is the least of the problems that IPv6 adoption should be concerned with.

DNS Fragmentation

At least one major attempt will be made to create an alternative DNS, backed by a government or state. Additionally, at least one large-scale commercial venture will do the same. The government entity may succeed, but the commercial venture will fail unless it is also backed by a major government, if for nothing more than sheer lack of profit, unless it fulfills a specific niche market, such as some network built on the Internet for a special purpose such as high security. Alternatively, attempts by governments to control DNS and the Internet, such as copyright-related domain name seizures executed by the United States in 2011 [Kravets, 2011] or attempts to seal off parts of the Internet in politically volatile regions [Greenemeier, 2011], may lead to the adoption of a peer-to-peer based DNS system, with at least one project garnering significant interest after only a short time [Greere, 2010]. This approach would be considerably more difficult to force into compliance by any government and, much like faith-based currency, may become more influential than the "traditional" DNS if it is considered more valuable and adopted by the majority of Internet users.

The DNS Architecture Will Remain a Standard

If IPv4 to IPv6 conversion is difficult, converting from DNS to a completely new system will probably not be much better, and have far fewer short-term benefits that are visible to the end user. Any changes will have to be client-transparent, as there is far too much software written with DNS in mind to make a switchover feasible except in the most extreme circumstances. IPv6 DNS is designed to address many of these issues, so if and when the conversion of the main Internet to IPv6 is activated, many flaws should, with luck, become irrelevant [Carli, 2003].

Third Party Registrar Corruption Will Reach Critical Levels

Third party registrars do not seem to have the same spirit of community that helped to build the Internet from scratch. Although it is arguable that organizations like ICANN are no longer in possession of this quality, it is more likely that they at least retain some of the cultural mindset within the organization, not to mention some of the veterans; as such, many of the lower-level, third party registrars will continue to attempt to extract as much profit from their position as possible, even at the possible long-term detriment of the Internet at large. Eventually there will likely be some critical turning point that leads to heavy reevaluation of the entire system.

UDRP Will Change Significantly

The UDRP has worked so far, but not without problems. Some shortcomings of the procedure include requisite "bad faith" is ill-defined; complaining parties (often trademark holders) seem to have bias in their favor; the UDRP is not legal arbitration nor binding, allowing litigious intervention; parties such as large, corporate interests can more easily afford associated costs; and English dominates the process [Diéguez, 2008]. The UDRP has existed for over a decade [InterNIC, 2002b], providing sufficient experience to learn where it needs improvement [Diéguez, 2008]. Given the increase in corporate influence on the Internet, as well as public awareness, it is likely that there may be a struggle, with corporate interests gaining the upper hand and possible changes due to backlash; however, given the legal position of the UDRP, it may ultimately end up a supplement to the court system as opposed to an attempt at manifesting a final authority as originally intended.

Increasing Governmental Influence

As of 2011, legislative action in several countries has indicated that DNS may encounter influence by governments as a method of filtering out undesirable Internet sites, as a result of pressure from both political and corporate forces. This may create considerable problems for its continued acceptance as a standard, as it is likely that the marketplace will gain support for a replacement resistant to external changes, regardless of its legality [Bambauer, 2011]. Such competition may place considerable strain on the primary implementation of DNS to remain relevant

IPR2025-01400
CrowdStrike EX1021 Page 11

and address the needs of many on the Internet, though it may be questionable how much support such a shift in naming technology could actually gather if it should retain a reputation as contraband or be challenging for a user to install and utilize. It may also endure the abuses DNS already struggles with, as well as additional, unanticipated abuses that may accompany any new technology used in potential replacements. Although highly unlikely, a worst-case scenario may result in a period of considerable ambiguity if no single DNS implementation maintains universal global acceptance.

DNS Will Never Be Perfect

Almost all systems have flaws. Even if the oft-cited IPv6 version of DNS corrects all the major structural flaws in the IPv4-based DNS, it remains under the radar and relatively new, whereas IPv4 DNS is ubiquitous and has been around for over two decades for analysis and dissection by would-be attackers. Furthermore, national governments will always squabble, as will agencies that govern systems like the DNS, whether they are government backed, corporate backed, independent, or otherwise. Ultimately, there will always be problems with the DNS, even if we fix all of those that are in existence; it is, in the end, a never-ending cycle, which, with luck, will continue to induce a net strengthening of the system as a whole.

V. FUTURE RESEARCH

DNS has always been a critical part of the Internet's modern infrastructure. While it replaced the simpler system of HOSTS.TXT and may one day be replaced itself, there will always be a need for a directory service to translate complicated network identification into a readily human-readable format. As such, it is important that the development of DNS be monitored and studied. DNS is unique in the demands that are placed upon it—whereas many other Internet protocols and systems are far more independent of government and cultural influences, DNS must represent these. With the increase in the proliferation of the Internet, the larger network population and stronger commercial influence also place demands on DNS. The influences that may affect DNS research and development are also in flux—while that of the international community is on the rise, the exclusive power of the United States government over its regulation and administration is waning, and technological limitations that would have at one time proven insurmountable will increasingly become tractable problems.

A research model is proposed to guide future study of the influence between DNS as it evolves, as well as the external factors, several of which have been discussed in this article. This model, illustrated in Figure 3, includes the impact of influences increasing in power, both socioeconomic and governmental, as well as those decreasing in power, such as those of the U.S. government and technological limitations. It also encapsulates the learning and research process and how it coexists with technological development, and how this is applied to DNS as it evolves. This model is only a rough approximation; further research into validation of this model or other models like it may prove as valuable guidance in the future development of DNS and large systems with similarly diverse requirements and stakeholders involved. Particularly valuable venues may include in-depth study as to the change in the balance of power over DNS development and administration, as well as the influence that DNS has had over research and, in turn, technological adaptations.

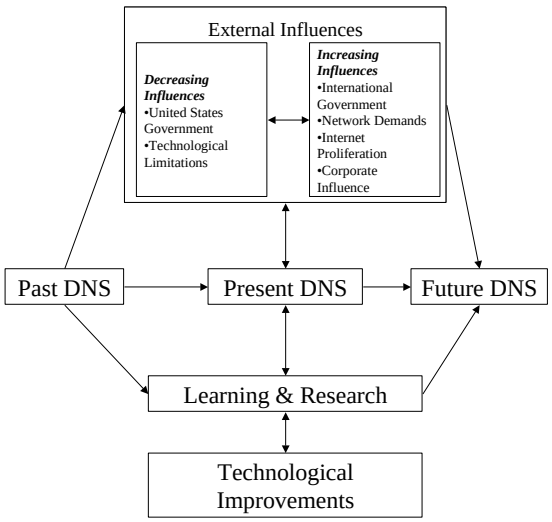

Figure 3. Proposed Model of DNS Development Over Time

IPR2025-01400
CrowdStrike EX1021 Page 12

The application of this model, even in hypothetical form, may be useful for many aspects of DNS research. One example of this is the push for a true peer-to-peer DNS. A tactic often employed by governments to exercise influence on DNS is to prevent the system from delivering information regarding an undesired domain name, usually providing content that is considered illegal or objectionable [Zittrain and Edelman, 2003]. This would also be effective, at least in some cases, at disrupting communication within different parts of a website or interactions between interconnected websites, as often their data and programs embed domain names instead of IP addresses, for maximum flexibility, and may be impractical to implement using only numerical addresses. A true peer-to-peer solution would likely be able to bypass this. It could be implemented in different ways; for example, by making the DNS a locally-stored database and with data passed between nodes automatically, a user could administrate his or her own DNS entries, updating without necessarily going through an influenced central authority. Alternatively, a mesh-style network could be implemented with different parts of the database shared between peers, reducing storage requirements on less powerful machines. It is likely that unwanted changes would be detected and corrected in short order. As of 2011, proposed legislation in the United States and other countries is likely to increase interest in this type of system, as well as other, alternative DNS systems [Bambauer, 2011], particularly in light of movements such as the so-called Arab Spring, involving considerable political changes in the Middle East. The model may be used to better understand how DNS reacts to these changes in the context of its development, examination of these new systems using DNS as a basis, and comparative studies between DNS and potential competitors, both for alternate implementations of the conventional DNS system as well as new technologies.

On an international level, the influence of the United States on the Internet, while still strong, is far from a given or constant. Studies on the effects of these changes, at least when examining the Internet infrastructure as a whole, would likely include DNS, due to its vital enabling role. Impacts in the political science realm may be felt as this changing balance manifests in diplomatic relations and treaties, resulting in changing international relations, as well as changing relations between multi-national organizations. It would behoove researchers studying sociopolitical aspects of the Internet and its international impact at large to consider this model and to expand on it, as well as to provide context from the culture of the Internet itself and that of countries competing for this influence.

Societal changes may also impact on DNS. The very organization of DNS involves hierarchies which may very subtly have a psychological influence which varies between societies. Changes in the actual names available, with the introduction of non-Latin characters, may also allow for a culture to express itself more distinctly—countries and cultures that use different character sets for their predominant language may be able to express their identities more distinctively by enabling more familiar names, and may convey additional information through them that might not be adaptable through a foreign character set. The proposed model allows for a greater perspective of the technological part of this dynamic as it changes.

All of these aspects may ultimately influence the design of DNS itself. A core component of IS scholarship consists of explorations of how users interact with technology, and DNS is a major enabling technology. Learning about the sociology and psychology surrounding DNS is key to adapting it to changing needs, which is vital as technology and society changes. Understanding what has worked in the past, what has not worked, and how it has interacted with the Internet ecology around it is fundamental to keeping it sufficiently well-adapted to rapidly changing technological capabilities and standards, and assisting efforts to design technical solutions in the future.

VI. CONCLUSIONS

For the DNS to continue to provide its vital services to future Internet users, these challenges must be effectively addressed by the international community of users. The perspective of each stakeholder group—users, domain owners, webmasters, governments, and others—must be considered in the decisions about the design and administration of the DNS. Ongoing security challenges must also be faced, and creative solutions to new security threats must be established for the continued benefit of all Internet users. Legislative action on the part of several governments have also created challenges for the continued relevance of DNS. The dynamic nature of the Internet ecology, technology, culture, and law warrant the continued study of DNS history in order to determine its future and the future of potential successors. We hope to have provided some insight as to the status of the DNS, how it came to be, and some thoughts on how it may change in the future; we hope we have provided a starting point for future research. Ultimately, these important decisions will require compromises and sacrifices so that we can all benefit from continued expansion of the Internet and its functionality.

ACKNOWLEDGMENTS

A previous version of this paper was presented at the 2009 National Decision Sciences Institute (DSI) Annual Conference where it was awarded Information Systems 2009 Distinguished Paper.

IPR2025-01400
CrowdStrike EX1021 Page 13

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Aaron, G., and R. Rasmussen (2010) "Global Phishing Survey: Trends and Domain Name Use 2H2009," *The Anti-Phishing Working Group*, http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf (current July 9, 2010).

Abolins, J.D. (2010) "This Domain Name Is Greek to Me: An Introduction to Internationalized Domain Names for Investigators," *Digital Forensic Investigator News*, http://www.dfinews.com/article/domain-name-greek-me-introduction-internationalized-domain-names-investigators (current July 9, 2010).

Adler, P., et al. (1994) "InterNIC Midterm Evaluations and Recommendations—A Panel Report to the National Science Foundation," http://www.codeontheroad.com/papers/InterNIC.Review.pdf (current June 8, 2011).

Alexander, T. (2006) "Domain Name Registrars: Are They Part of the Domain Name Fraud Problem?" *Proceedings of InfoSecCD 2006*, New York, NY: ACM Press.

Bambauer, D. (2011) "De-lousing E-PARASITE," *Info/Law,* http://blogs.law.harvard.edu/infolaw/2011/11/05/de-lousing-e-parasite/ (current Nov. 6, 2011).

Bambauer, D.E. (2011) "Orwell's Armchair," *University of Chicago Law Review*, forthcoming, http://ssrn.com/abstract=1926415 (current Nov. 6, 2011).

Berlind, D. (2003) "DNS Inventory Says Cure to Net Identify Problems Is Right Under Our Nose," *ZDNet.com*, http://www.zdnet.com/news/dns-inventor-says-cure-to-net-identity-problems-is-right-under-our-nose/296225?tag=content;search-results-rivers (current June 5, 2011).

Berners-Lee, T. (1996) "WWW: Past, Present and Future," *Computer* (29)10, pp. 69–77.

Blue, V. (2011) ".XXX Domain Approved: Now Begins the Era of Meaningless TLDs," *ZDNet.com*, http://www.zdnet.com/blog/violetblue/xxx-domain-approved-now-begins-the-era-of-meaningless-tlds/280?tag=nl.e539 (current May 21, 2011).

Bose, I., and A.C.M. Leung (2007) "Unveiling the Mask of Phishing; Threats, Preventive Measures, and Responsibilities," *Communications of the Association for Information Systems* (19) Article 24, pp. 544–566.

Borland, J. (2003) "Victor: Software Empire Pays High Price," *CNet News*, http://news.cnet.com/2009-1032-995681.html (current Mar. 17, 2009).

Borland, J., P. Festa, D. Becker, and M. Yamamoto. (2003) "How the Mosaic Browser Triggered a Digital Revolution," *CNet News*, http://news.cnet.com/2009-1032-995679.html (current Mar. 17, 2009).

Bryant, N. (2008) "Australia Trials National Net Filters," *BBC News,* http://news.bbc.co.uk/2/hi/technology/7689964.stm (current Mar. 30, 2009).

Carli, F. (2003) "Security Issues with DNS," *SANS Institute InfoSec Reading Room*, http://www.sans.org/reading_room/whitepapers/dns/security_issues_with_dns_1069?show=1069.php&cat=dns (current Jan. 8, 2009).

Cerf, V.G. (1995) "Computer Networking: Global Infrastructure for the 21st Century," *University of Washington Computer Science & Engineering*, http://www.cs.washington.edu/homes/lazowska/cra/networks.html (current Mar. 8, 2009).

Cheng, J. (2011) "ICANN Approves .XXX Red-light District for the Interne,t, *Ars Technica*, http://arstechnica.com/tech-policy/news/2011/03/icann-approves-xxx-red-light-district-for-the-internet.ars (current May 21, 2011).

Davis, K., and M. Warkentin (2001) "Strategic and Legal Issues in Internet Branding: Selection and Protection of Internet Domain Names," *Proceedings of the National Decision Sciences Institute (DSI) 32nd Annual Conference*, San Francisco, CA, Nov. 17–20, 2001, Atlanta, GA: Decision Sciences Institute, pp. 246–248.

IPR2025-01400
CrowdStrike EX1021 Page 14

Deegan, T., C. Crowcoft, and A. Warfield (2005) "The Main Name System: An Exercise in Centralized Computing," *ACM SIGCOMM Computer Communication Review* (35)5, pp. 5–13.

Diéguez, J.P.C. (2008) "An Analysis of the UDRP Experience: Is it Time for Reform?" *Computer Law and Security Review* (24)10, pp. 349–359.

DomainNameStuffetc.com (2002) "Domain Names Big Money," http://www.domainnamestuffetc.com/big_money.htm (current Mar. 17, 2009).

Edmondson-Yurkanan, C. (2007) "Journey into Networking's Past: Documenting the Technical History of a SIG is Indeed a Priceless Resource," *Communications of the ACM* (50)5, pp. 63–67.

EDUCAUSE (2009) "EDUCAUSE .edu Home Page," http://net.educause.edu/edudomain/ (current Mar. 30, 2009).

Elias, S., and R. Stim (2007) *Trademark: Legal Care for Your Business and Product Name, 8th edition,* Berkeley, CA: Nolo, p. 249.

Espiner, T. (2008) "DNS Creator: It's Time to Add Security," *ZDNet.com*, http://news.zdnet.co.uk/security/0,1000000189,39459935,00.htm (current Mar. 30, 2009).

Foner, L. (2001) "Fixing a Flawed Domain Name System," *Communications of the ACM* (44)1, pp. 19–21.

Fuller, K.E. (2001) "ICANN: The Debate over Governing the Internet," *Duke Law & Tech Review*, http://www.law.duke.edu/journals/dltr/articles/2001dltr0002.html (current Mar. 30, 2009).

Fulton, M. (2008) "Domain Tasting Goes Sour: ICANN Will No Longer Issue Registration Refunds," *DotSauce*, http://www.dotsauce.com/2008/01/29/the-end-of-domain-tasting (current Jan. 8, 2009).

Gabrilovich, E., and A. Gontmakher (2002) "The Homograph Attack," *Communications of the ACM* (45)2, pp. 128–129.

Garrison, S. (2011) "7 Must Have Attributes of an IP Address Management System," *CircleID*, http://www.circleid.com/posts/20110418_7_must_have_attributes_of_an_ip_address_management_system/ (current June 7, 2011).

Greenemeier, L. (2011) "How Was Egypt's Internet Access Shut Off?" *Scientific American*, Jan. 28, http://www.scientificamerican.com/article.cfm?id=egypt-internet-mubarak (current June 20, 2011).

Greere, D. (2010) Peter Sunde Starts Peer-to-peer DNS System, *Wired*, http://www.wired.co.uk/news/archive/2010-12/02/peter-sunde-p2p-dns (current June 20, 2011).

Guice, J. (1998) "Looking Backward and Forward at the Internet," *The Information Society* (14), pp. 201–211.

Hachman, M. (2011) "Generic TLD Process to be Finalized in June," *PCMagazine*, http://www.pcmag.com/article2/0,2817,2382233,00.asp (current May 21, 2011).

Harvard University (2000) "Brief History of the Domain Name System," *Berkman Center for Internet & Society*, http://cyber.law.harvard.edu/icann/pressingissues2000/briefingbook/dnshistory.html (current Mar. 8, 2009).

Healey, C. (2007) "Domain Tasting Is Taking over the Internet as a Result of ICANN's 'Add Grace Period,'" *Duke Law and Technology Review*, http://www.law.duke.edu/journals/dltr/articles/2007DLTR0009.html (current Sept. 5, 2009).

Held, G. (2002) *The ABCs of IP Addressing*, Boca Raton, FL: CRC Press LLC.

Hogge, B. (2008) "The Great Phonebook in the Sky," *New Statesman*, 137(4883), p. 50.

Hovav, A., and D. Schuff (2005) "Global Diffusion of the Internet V—The Changing Dynamic of the Internet: Early and Late Adopters of the IPv6 Standard," *Communications of the Association for Information Systems* (15) Article 14, pp. 242–262.

IANA (2009) "Number Resources," *Internet Assigned Numbers Authority*, http://www.iana.org/numbers/ (current Mar. 17, 2009).

ICANN (2000) "Chronological History of ICM's Involvement with ICANN," *Internet Corporation for Assigned Names and Numbers*, http://www.icann.org/en/irp/icm-v-icann/icm-icann-history-21feb10-en.pdf (current July 9, 2010).

ICANN (2006) "ICANN Board Votes Against .XXX Sponsored Top Level Domain Agreement," *Internet Corporation for Assigned Names and Numbers*, http://www.icann.org/en/announcements/announcement-10may06.htm (current Jan. 8, 2009).

ICANN (2007) "ICANN FAQ," *Internet Corporation for Assigned Names and Numbers*, http://www.icann.org/en/faq/ (current Jan. 8, 2009).

IPR2025-01400
CrowdStrike EX1021 Page 15

ICANN (2008a) "Biggest Expansion in gTLDs Approved for Implementation," *Internet Corporation for Assigned Names and Numbers,* http://www.icann.org/en/announcements/announcement-4-26jun08-en.htm (current Jan. 8, 2009).

ICANN (2008b) "Top-Level Domains (gTLDs)," *Internet Corporation for Assigned Names and Numbers*, http://www.icann.org/en/tlds/ (current Mar. 17, 2009).

ICANN (2008c) "About," *Internet Corporation for Assigned Names and Numbers*, http://www.icann.org/en/about/ (current Mar. 17, 2009).

ICANN (2008d) "New gTLD Program: Draft Applicant Guidebook (Draft RFP)," *Internet Corporation for Assigned Names and Numbers*, http://www.icann.org/en/topics/new-gtlds/draft-rfp-24oct08-en.pdf (current Mar. 30, 2009).

ICANN (2009) "The End of Domain Tasting," http://www.icann.org/en/announcements/announcement-12aug09-en.htm (current Sept. 5, 2009).

ICANN (2011) "ICANN Approves Historic Change to Internet's Domain Name System," http://www.icann.org/en/announcements/announcement-20jun11-en.htm (current June 23, 2011).

IETF (2009) "IETF Home Page," *The Internet Engineering Task Force*, http://www.ietf.org/ (current Mar. 8, 2009).

InterNIC (2002a) "InterNIC FAQs: The Domain Name System: A Non-Technical Explanation—Why Universal Resolvability Is Important," *InterNIC*, http://www.internic.net/faqs/authoritative-dns.html (current Mar. 9, 2009).

InterNIC (2002b) "InterNIC FAQs on the Uniform Domain Name Dispute Resolution Policy (UDRP), *InterNIC*, http://www.internic.net/faqs/udrp.html (current Sept. 1, 2009).

Johanson, E. (2005) "The State of Homograph Attacks," *The Shmoo Group*, http://www.shmoo.com/idn/homograph.txt (current July 9, 2010).

Kaminsky, D. (2008) "It's the End of the Cache as We Know It, or: '64K Should Be Good Enough for Anyone,'" *Black Hat 2008*, http://www.doxpara.com/DMK_BO2K8.ppt (current Mar. 30, 2009).

Kravets, D. (2011) "U.S. Faces Legal Challenge to Internet-Domain Seizures," *Wired*, June 13, http://www.wired.com/threatlevel/2011/06/domain-seizure-challenge/ (current June 23, 2011).

Lee, D.C., et al. (1998) "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6," *IEEE Network* (12)1, pp. 28–33.

MaxMind (2011) "Allocation of IP addresses by Country," *MaxMind,* http://www.maxmind.com/app/techinfo (current Nov. 5, 2011).

Mockapetris, P.V., and K.J. Dunlap (1995) "Development of the Domain Name System," *ACM SIGCOMM Computer Communications Review* (25)1, pp. 112–122.

Mohan, R. (2011) "DNSSEC Deployment Reaching Critical Mass," *CircleID.com*, http://www.circleid.com/posts/20110321_dnssec_deployment_reaching_critical_mass/ (current June 6, 2011).

Mueller, M.L. (1997) "Internet Domain Names Privatization Competition and Freedom of Expression," *CATO Institute Briefing Papers*, http://www.cato.org/pubs/briefs/bp-033.html (current Mar. 17, 2009).

Neylon, M. (2010) "IDN Scaremongering: Mashable and Times Online Screw Up," *CircleID*, http://www.circleid.com/posts/idn_scaremongering_mashable_and_times_online_screw_up/ (current July 9, 2010).

NSF (1995) "The Internet Grows Up," *Office of Legislative and Public Affairs (OLPA) News*, http://www.nsf.gov/news/news_summ.jsp?cntn_id=100806&org=olpa&from=news (current Mar. 30, 2009).

NSF (2009) "The Internet: Changing the way we communicate," *National Science Foundation*, http://www.nsf.gov/about/history/nsf0050/pdf/internet (current Mar. 8, 2009).

OpenNIC (2009) "Welcome to the OpenNIC Project," *OpenNIC*, http://www.opennicproject.org (current Jan. 8, 2009).

Oversee.net (2010) "Increasing the Value of Internet Real Estate," *Oversee.net*, http://www.oversee.net/ (current July 9, 2010).

Parsons, B. (2006) "35 Million Names Registered in April. 32 Million Were Part of a Kiting Scheme. A Serious Problem Gets Worse," *Bob Parson Blog Archive*, http://www.bobparsons.me/117/35-million-names-registered-april-32-part-kiting-scheme-serious-problem-gets-worse.html (current Mar. 30, 2009).

IPR2025-01400
CrowdStrike EX1021 Page 16

Postel, J., and J. Reynolds (1984) "Domain Requirements—RFC 920," *The Internet Engineering Task Force*, http://tools.ietf.org/html/rfc920 (current Jan. 8, 2009).

Prince, B. (2008) "DNS Flaw Leaves Major Internet Security Hole," *eWeek*, http://www.eweek.com/c/a/Security/DNS-Flaw-Leaves-Major-Internet-Security-Hole/ (current Nov. 11, 2008).

Public-Root (2009) "Welcome to the Public-Root," *Public-Root*, http://public-root.com (current Jan. 8, 2009).

Ramasubramanian, V., and E.G. Sirer (2004) "The Design and Implementation of a Next Generation Name Service for the Internet," *Proceedings of SIGCOMM 2004*, New York, NY: ACM Press.

Rashid, F.Y. (2011) "ICANN Approves Custom Generic Top Level Domains," *eWeek,* http://www.eweek.com/c/a/Cloud-Computing/ICANN-Approves-Custom-Generic-Top-Level-Domains-775234/ (current Nov. 5, 2011).

Rogers, J.D. (1998) "Internetworking and the Politics of Science: NSFNET in Internet History," *The Information Society* (14), pp. 213–228.

Sayer, P. (2010) "Chinese Language Top-level Domains Win ICANN Approval," *Computerworld*, http://www.computerworld.com/s/article/9178525/Chinese_language_top_level_domains_win_ICANN_approval (current June 25, 2010).

Shankland, S. (2011) "New Net Addresses Mean New Trademark Issues," *CNet DeepTech*, http://news.cnet.com/8301-30685_3-20072470-264/new-net-addresses-mean-new-trademark-issues/ (current June 20, 2011).

Sun (2009) "Brief History of the Domain Name System," *Sun Microsystems*, http://www.sun.com/hardware/serverappliances/pdfs/support/dns.history.pdf (current Mar. 8, 2009).

UnifiedRoot (2009) "Top Level Domain Registration," *UnifiedRoot*, http://www.unifiedroot.com (current Jan. 8, 2009).

US-CERT (2008) "Vulnerability Note VU#800113—Multiple DNS Implementations Vulnerable to Cache Poisoning," *United States Computer Emergency Readiness Team*, http://www.kb.cert.org/vuls/id/800113 (current Jan. 8, 2009).

Vaughan-Nichols, S.J. (2010) "Practice Safe DNS," *ZDNet.com*, http://www.zdnet.com/blog/networking/practice-safe-dns/260?tag=content;search-results-rivers (current June 6, 2011).

Warkentin, M. (1999) "Protect Your Name! Web Strategy Tip," *Tech New England*, http://html.thebostonchannel.com/bos/technology/technewenglandarticles/stories/technewengland-20000907-085013.html (current Sept. 22, 2009).

Warner, B. (2007) "A Geriatric Assault on Italy's Bloggers," *Times Online*, http://technology.timesonline.co.uk/tol/newstech_and_web/the_web/article2732802.ece (current Jan. 8, 2009).

Wattanajantra, A. (2008) "Kaminsky's DNS Vulnerability," *ITPRO*, http://www.itpro.co.uk/605520/timeline-kaminsky-s-dns-vulnerability (current Mar. 6, 2009).

White, A. (2010) "Porn Sites Closer to .xxx Web Addresses," *The Associated Press*, http://www.google.com/hostednews/ap/article/ALeqM5jkXAgQJCO8KRyhLleJNZ7fa1gKdgD9GICCK81 (current June 25, 2010).

WIPO (n.d.) "WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)," *WIPO ADR*, http://www.wipo.int/amc/en/domains/guide/index.html (current Sept. 5, 2009).

Yamamoto, M. (2003) "Legacy: A Brave New World Wide Web," *CNet News*, http://news.cnet.com/2009-1032-995680.html# (current Mar. 17, 2009).

Zittrain, J., and B. Edelman (2003) "Internet Filtering in China," *IEEE Internet Computing* (7)2, pp. 70–77.

IPR2025-01400
CrowdStrike EX1021 Page 17

ABOUT THE AUTHORS

Michael Brian Pope is a doctoral candidate in MIS at Mississippi State University. He holds a bachelor's and master's degree in computer science from California State University, Sacramento. His current research interests include telecommunication, security, social media, knowledge management, and the legal aspects of IS. His work has been published in *Communications of the Association for Information Systems* and in the *Proceedings of the Decision Sciences Institute* annual conference, where it was nominated for best paper.

Merrill Warkentin is a professor of MIS and the John and Carole Ferguson Notable Scholar at Mississippi State University. He earned his Ph.D. in MIS at the University of Nebraska-Lincoln. His research focuses on behavioral issues in IS Security and electronic group collaboration. He has authored over 250 manuscripts and six books. He is serving as Associate Editor for *MIS Quarterly*, *European Journal of Information Systems*, and *Information & Management*. He has chaired several international conferences, including IFIP and WISP. His work has been supported by the U.S. Navy, NSA, the IRS, the UN, Homeland Security, IBM, and others. He has been a visiting scholar at over two dozen universities in eight nations, and has served as an ACM National Distinguished Lecturer. His work has appeared in *MIS Quarterly*, *Decision Sciences*, *European Journal of Information Systems*, *Decision Support Systems*, *DATA BASE for Advances in Information Systems*, *Information Systems Journal*, *Communications of the Association for Information Systems*, *Communications of the ACM*, and other journals and in numerous books.

Leigh A. Mutchler is currently a doctoral candidate and lecturer in MIS at Mississippi State University's College of Business. She holds a B.S. degree in Mechanical Engineering from the University of Memphis. Her primary research interests include IS Security, Computer Mediated Communications, and Knowledge Management.

Xin (Robert) Luo is an associate professor of MIS and Information Assurance in the Anderson School of Management at The University of New Mexico. He received his Ph.D. in MIS from Mississippi State University. His research interests center around information security, innovative technologies, and cross-cultural IT management. His research articles have appeared in leading journals such as *Journal of the Association for Information Systems, European Journal of Information Systems, Decision Support Systems, Communications of the ACM, Journal of Strategic Information Systems,* and *Communications of the Association for Information Systems,* among others. He is an Associate Editor for ICIS 2011 and a special issue on cross-cultural studies of *European Journal of Information Systems*.

IPR2025-01400
CrowdStrike EX1021 Page 18

Copyright © 2012 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712, Attn: Reprints; or via e-mail from ais@aisnet.org.

IPR2025-01400
CrowdStrike EX1021 Page 19

Communications of the Association for Information Systems

ISSN: 1529-3181

EDITOR-IN-CHIEF
Ilze Zigurs
University of Nebraska at Omaha

AIS PUBLICATIONS COMMITTEE

Kalle Lyytinen Vice President Publications Case Western Reserve University	Ilze Zigurs Editor, *CAIS* University of Nebraska at Omaha	Shirley Gregor Editor, *JAIS* The Australian National University
Robert Zmud AIS Region 1 Representative University of Oklahoma	Phillip Ein-Dor AIS Region 2 Representative Tel-Aviv University	Bernard Tan AIS Region 3 Representative National University of Singapore

CAIS ADVISORY BOARD

Gordon Davis University of Minnesota	Ken Kraemer University of California at Irvine	M. Lynne Markus Bentley University	Richard Mason Southern Methodist University
Jay Nunamaker University of Arizona	Henk Sol University of Groningen	Ralph Sprague University of Hawaii	Hugh J. Watson University of Georgia

CAIS SENIOR EDITORS

Steve Alter University of San Francisco	Michel Avital Copenhagen Business School	Jane Fedorowicz Bentley University	Jerry Luftman Stevens Institute of Technology

CAIS EDITORIAL BOARD

Monica Adya Marquette University	Dinesh Batra Florida International University	Indranil Bose Indian Institute of Management Calcutta	Thomas Case Georgia Southern University
Evan Duggan University of the West Indies	Andrew Gemino Simon Fraser University	Matt Germonprez University of Wisconsin-Eau Claire	Mary Granger George Washington University
Åke Gronlund University of Umea	Douglas Havelka Miami University	K.D. Joshi Washington State University	Michel Kalika University of Paris Dauphine
Karlheinz Kautz Copenhagen Business School	Julie Kendall Rutgers University	Nelson King American University of Beirut	Hope Koch Baylor University
Nancy Lankton Marshall University	Claudia Loebbecke University of Cologne	Paul Benjamin Lowry City University of Hong Kong	Don McCubbrey University of Denver
Fred Niederman St. Louis University	Shan Ling Pan National University of Singapore	Katia Passerini New Jersey Institute of Technology	Jan Recker Queensland University of Technology
Jackie Rees Purdue University	Raj Sharman State University of New York at Buffalo	Mikko Siponen University of Oulu	Thompson Teo National University of Singapore
Chelley Vician University of St. Thomas	Padmal Vitharana Syracuse University	Rolf Wigand University of Arkansas, Little Rock	Fons Wijnhoven University of Twente
Vance Wilson Worcester Polytechnic Institute	Yajiong Xue East Carolina University		

DEPARTMENTS

Information Systems and Healthcare Editor: Vance Wilson	Information Technology and Systems Editors: Dinesh Batra and Andrew Gemino	Papers in French Editor: Michel Kalika

ADMINISTRATIVE PERSONNEL

James P. Tinsley AIS Executive Director	Vipin Arora CAIS Managing Editor University of Nebraska at Omaha	Sheri Hronek CAIS Publications Editor Hronek Associates, Inc.	Copyediting by S4Carlisle Publishing Services

Communications of the Association for Information Systems

IPR2025-01400
CrowdStrike EX1021 Page 20