

IGF 2016 Workshop Report Template

Session Title	WS 75 Domain Name System fragmentation? Risk and reality
Date	9 December, 2016 (Friday)
Time	12:00 – 13:30
Session Organizer	Milton Mueller and Farzaneh Badii
Chair/Moderator	Dr. Milton Mueller
Rapporteur/Notetaker	Arvin Kamberi
List of Speakers and their institutional affiliations	<p>Badii, Farzaneh, IGP, Georgia Tech Demidov, Oleg, PIR Center, Russia Kuerbis, Brenden, IGP, Georgia Tech Ranjbar, Kaveh, RIPE-NCC Shea, Ryan, Blockstack Ali, Muneeb, Blockstack Song, Davey, Beijing Internet Institute Sullivan, Andrew, Fellow at Dyn, Internet Architecture Board Vixie, Paul, Farsight Security</p>
Key Issues raised (1 sentence per issue):	<ol style="list-style-type: none"> 1. What is the possibility of a major split in DNS caused by geopolitical differences? 2. Does the YETI experiment with an alternate DNS root for scientific research risk fragmenting the root? 3. Has convergence on a common DNS stifled innovation in naming? How do we reconcile new DNS and naming technologies with global compatibility?
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	<p>Oleg Demidov of the PIR Center, said that Russian government concerns about the possible instability of the national segment of the DNS began in 2014. A study to test the resilience and stability of the Russian Internet was conducted. All critical scenarios were included in the study, including the possibility of US deleting ccTLDs to another failure or modification related to the Russia ccTLD in the global root zone file. Of all models, a major failure in the global DNS had the lowest probability of occurrence. Even with the low possibility, this scenario might have critical consequences, so Russian regulatory bodies set in motion a set of policies to provide the backup of information related to all of the domains and names in the Russian domain name system, which will give them ability to replicate them on local servers in the case of a major failure or disruption in the global DNS. This is not the case of a fragmentation of the DNS but rather a redundancy issue, he added. The probability of a major split in the DNS root is very low.</p> <p>Ms Farzaneh Badii, Executive Director of the Internet Governance Project, discussed the court case concerning the ccTLD .IR, the country code for Iran. A group of terrorism victims gained a</p>

monetary judgment against the state of Iran using US law. Since Iran does not have any other assets in the USA, they brought a civil lawsuit against ICANN based on the premise that .IR is a property asset that could be seized and its value used to compensate the victims. ICANN refused the request, stating that a ccTLD is not a property. The latest court judgment stated that allowing the Israeli terrorism victims to seize the .IR domain would impair ICANN's interest in protecting the stability and interoperability of the Internet. There was a fear that taking a country code away from a government based on litigation might lead to a defection of the affected state from the ICANN regime. In other words, the decision was based not on the domain's property status but on geopolitical concerns about fragmenting the DNS.

Discussion on alternative technical solutions started with a presentation by Mr Paul Vixie, Internet pioneer and innovator, involved in the creation of the current DNS. He presented the YETI-DNS project, which is a 'parallel experimental live IPv6 DNS root system to discover the limits of the DNS root name service'. He stated that YETI is not intended to bifurcate or amend the global root and existing IANA namespace. He stated that whatever you're going to do on the Internet, in order to be relevant and successful, it has to be in cooperation with the other people on the Internet. Project YETI is showing that the DNS can be fragmented, even with DNSSEC in place, and goes in the direction of national or even regional splitting of the DNS. Anyone could create a parallel system that was powered completely by the optimal cooperation of the people who were publishing and subscribing, he noted. Vixie added that reason why other alternative domain name systems have failed can be found in IANA's ability to cooperate, for example its ability to eventually allow for the creation of new gTLDs. ICANN has always been open to the community. As long as it continues this way, IANA is not in danger.

Mr Kaveh Ranjbar, Chief Information Officer, RIPE NCC, indicated that a project like YETI should not be considered to be like the Internet, but rather Internet technology. The Internet Engineering Task Force (IETF) is the glue that keeps the Internet together, he added. If it does not come from the IETF, we should not consider it to be a fragmentation, but rather an experiment within the Internet infrastructure. If the IETF were voting on a new RFC stating that a resolver can use more than one address for routing, that's what he would consider to be Internet fragmentation, he added.

Mr Andrew Sullivan, Director of DNS Engineering, Dyn, pointed out that the magic of the Internet is that it's a collaborative effort, shown by the fact that all individual networks share some common pathways, so that they work together. No authority is in the middle. This allows arbitrary connections between people without anybody's permission, in addition to other forms of permissionless

	<p>innovation. He mentioned .local or .onion which are parts of the hierarchical name space, but not in DNS. There is technical resistance to fragmentation, as well as a practical resistance to fragmentation. It is in everybody's self-interest to have a unique name space.</p> <p>Mr Brenden Kuerbis, Postdoctoral Researcher, Internet Governance Project, Georgia Institute of Technology, pointed out that a good path would be to focus on creating institutions promote the security and stability of the DNS, while continuing to foster innovation of the core infrastructure. The institutionalization of a networked governance structure in the Public Technical Identifiers (PTI) organization, that involves all the communities and leads to a mutually beneficial outcome, is one pertinent example. It allows anyone to innovate a complementary or competing naming system, and be assured that a request for a globally compatible identifier will be satisfied by the PTI. In this sense PTI serves as a non-discriminatory way of coordinating different namespaces.</p> <p>Mr Ryan Shea, Co-founder of Blockstack Labs, gave an overview of the idea behind Blockstack, that provides a DNS on a blockchain technology. It runs on top of Bitcoin's blockchain, and it offers a decentralised way of running an individual namespace. Users can create their own namespace, and set their configuration and parameters. He added that this is a flat name space, so there are no servers. Therefore it can be considered to be an alternate root where the security and the integrity of the data is backed up by blockchain. It is operational and there around 70,000 names registered. All names own public keys, so it is not necessary to acquire security certificates separately, he added. This could replace a hierarchical root service with a decentralized virtual hierarchy with no single place to attack to undermine the system.</p>
<p>Please describe the Discussions that took place during the workshop session: (3 paragraphs)</p>	<p>After hearing position statements workshop participants engaged in broad discussion on fragmentation, including special use names and alternative naming systems like Blockstack and the Digital Object Architecture (DOA).</p> <p>Technically, Blockstack could leverage the existing DNS (i.e., subdomains under blockstack.org) or pursue a special use name at IETF. Each solution presents different costs. The history of telecom interconnection provides lessons for interoperability and competition in naming systems. In telecom, smaller competing networks would seek to interconnect with existing larger networks to gain access to an installed user base.</p> <p>DOA was not generally seen as a fragmentation risk by the panelists. Debates over DOA represent institutional competition between ICANN and ITU. The DOA is not a competing but rather complementary naming system, as it provides persistent identifiers</p>

	<p>for digital object resources as opposed to DNS names which combine resources and location (host machines) data. As such, the DOA could be a useful naming system to certain groups, particularly intellectual property owners concerned with access to resources. However, this group is heavily vested in the existing DNS and ICANN, explaining some reluctance for the DOA system.</p> <p>Overall, the participants felt that the risk of geopolitical, technical or other fragmentation of the DNS was relatively low given the system's widespread use and associated network effects. The ability to innovate in the Internet's core is important to preserve and requires adequate governing structures.</p> <p>Video of the discussion is available at https://youtu.be/fMf3spUOmT8</p>
<p>Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)</p>	<p>Further institutionalization needs to happen in the IETF since it is the "policy making" body for special-use names used by alternative naming systems, and a contracting party with the PTI. Therefore, it can potentially act as a gatekeeper. Fortunately, the IETF appears to be revisiting RFC 6761 which provides guidance for the assignment of special use names. However, difficult questions remain regarding how naming system standards developed outside of the IETF should be treated.</p>