THE INTERNET'S ROOT OF POWER

by Dan Schiller

The *Financial Times* reports that in February 2007, Gregory Schulte, the U.S. ambassador to the International Atomic Energy Agency, urged the international community to use the "'measures at its disposal' to direct political, economic, communications and other… pressures at Iran's leadership."[1] Perhaps it is time to ask: Could the United States curtail Internet access by an entire nation or, at least, by its institutional leadership?

States worry about such a prospect. One example surfaced in 2005, when several countries "expressed concern that the U.S. government…could unilaterally…cut them off from the Internet."[2] Might their concerns be well-founded? We hear so often that this network of networks is uncontrollably decentralized: does the capacity even exist to interdict Internet access on a systematic basis?

Though it possesses no simple on-off spigot, the Internet's distinctive architecture does offer points at which the U.S. enjoys unique leverage to disable service almost anywhere across the entire system. Explaining why this is true requires some basic acquaintance with the Internet's technical plumbing and, in particular, with the logic of its Domain Name System.[3]

The Domain Name System (DNS)

The DNS incarnates a twenty-five year history that has been shaped and structured by U.S. interests.

Through the DNS, means were created to assign unique identifiers for each cooperating Internet network and interconnected computer resource, because without such unambiguous identifiers the Internet could not function as a reliable communications medium. Expressed to ordinary Internet users in linguistic form – www.uiuc.edu for example – these complex names are structured hierarchically from right to left. The far right-hand label (e.g., .edu) constitutes the top level domain (TLD); the portion of the name to the left of the TLD constitutes the second-level domain (e.g., .uiuc). Linguistic names are used partly because they are

easier for humans to remember, and partly because they can be made relatively stable while the numerical Internet (IP) addresses to which they correspond may be conveniently altered for various purposes.

Names are converted by the DNS into numerical Internet (IP) addresses: 128.174.254.29, for example, is presently the numerical address for www.uiuc.edu. Largely invisible to ordinary users, it is IP addresses that effectuate Internet communication. An address's numerals and dots uniquely denote particular Internet-enabled computer resources. When a URL is typed into an interconnected computer, the DNS works to resolve the address by consulting files for each hierarchical component from right to left.

The organizational complex that supplies identifiers to each and every Internet-enabled network and computer or appliance and that resolves IP address requests is also hierarchical. At its apex sits the so-called "root zone file" (RZF), which houses authoritative data about where on the Internet numerical addresses are stored for top-level domain names, as Milton Mueller explains:

> The root is the point of centralization in the Internet's otherwise thoroughly decentralized architecture. The root stands at the top of the hierarchical distribution of responsibility that makes the Internet work. It is the beginning point in a long chain of contracts and cooperation governing how Internet service providers and end users acquire and utilize the addresses and names that make it possible for data packets to find their destinations.[4]

Whoever defines the root zone file in turn establishes a foundation for the strategic exercise of power over the Internet. This power pivot is held today, as it has been from the beginning of the DNS in the early 1980s, by the U.S. Executive Branch, in concert with a contracting organization, IANA, the Internet Assigned Number Authority established in the early 1980s and now nested within ICANN – the Internet Corporation for Assigned Names and Numbers established in 1998. Among other functions, the Department of Commerce and ICANN through IANA coordinate the management and operation of the root zone file through a related set of thirteen root name server operators.[5] How does this opaque system function?

In response to queries, the root server operators supply data about where definitive address information is stored for top-level domains (TLDs). The Internet is arranged so that this RZF is regularly updated and redistributed; in 2007 the root server operators maintained more than 100 root servers located in dozens of countries around the world.[6] Because the address data contained in these servers are both heavily redundant and routinely circulated, even a catastrophic shutdown of the root name services would still only "gradually impair the ability of computers on the Internet to resolve names."[7]

Occupying the next step down on the DNS hierarchy are top-level domains, of which there are two basic types: generic and country code domains. So far, there have been authorized nineteen different generic domains (gTLDs), such as .com, .org, .mobi (which operate under somewhat different sets of rules and conditions). Authorized as well have been 264 country codes (ccTLDs), each of which is designated by a two-letter code in conformity with an International Standardization Organization listing.[8] The country code for Iran, .ir, is managed by the Institute for Studies in Theoretical Physics & Mathematics in Tehran.

GTLD and ccTLD data are fed to ICANN by diverse cooperating agencies. Some gTLDs are run by for-profit organizations, others by nonprofit groups; some are based in the U.S. and others elsewhere. Yet some glaring disparities invalidate any idea that all TLDs possess equal stature. One generic top-level domain – .com – held, along with .net, by a U.S. company – commands a substantial share of TLDs in use globally. During the late 1990s' worldwide surge in Internet use, the U.S. proprietor of .com and .net controlled 75% of the world's domain name registrations.[9] Country code registrations of late have grown quickly, but they comprise only about one-third of all TLD registrations. The take-up of ccTLDs, moreover, varies greatly from country to country. According to a recent account, "In Latin America and to a lesser extent in Europe, ccTLDs constitute a majority of the TLDs registered. In contrast, in North America and to a lesser extent in the Asia Pacific region, ccTLDs are a minority of the TLDs registered. This can largely be attributed to historical facts and the early and continuing adoption and popularity of gTLDs in the United States."[10]

The ascent of this dual system of TLDs underlines a sharp contrast between the Internet and the prior international telecommunications infrastructure. Unlike the country codes that were established for voice telephony, no one-to-one relation between top-level identifiers and nation states governs cyberspace. Users in each country instead employ different TLDs, only some of which may fall under national authority. Put differently: no matter whether a country actively supports a ccTLD, control over the RZF and over .com and to a lesser extent other gTLDs grants ICANN and its sponsors the ability to reach, de facto, far into its domestic social life. To this extent, conceptions of national sovereignty in communications are presently a dead letter.

Rerooting the DNS?

With this technical detail at hand, we may turn back to the question of whether the DNS might be used by United States authorities to cripple Internet access for nations deemed enemies. Reflecting the complicated arrangements described above, each component of the DNS hierarchy poses distinct issues.

Innumerable second-level domains and many ccTLDs, managed by varied organizations, do not fall within U.S. jurisdiction; for the most part, as a

result, they are not within the direct reach of U.S. strategic power. This does not signify, however, that ccTLDs are immune from danger. More on this momentarily.

In contrast, the gTLDs including, in particular, .com, lie within ICANN's purview. Of considerable additional significance, by far the most important gTLD, .com (as well as .net), is managed by a shadowy U.S. corporation, VeriSign. VeriSign provides routing support for every Web address ending with .com or .net around the world, a task that presently requires it to field "as many as 21 billion domain name system queries every day."[11] Links between this company and the U.S. military/intelligence complex are explicit. A top VeriSign executive serves as a member of the U.S. National Security Telecommunications Advisory Committee – an elite group that assists the Executive Branch in forming policy for this strategically vital infrastructure.

But by far the most basic and consequential U.S. power function pertains to the highest level of the DNS hierarchy: the root zone file. According to Mueller, "The content of the RZF is defined by ICANN and modifications are approved by the U.S. Department of Commerce. The root server operators merely take that information and answer DNS queries based on it."[12] In principle, the U.S. possesses the ability to edit or reprogram the RZF so as to cease meeting query requests for data about particular top-level domains.

Ten of the thirteen root name server operators are U.S. entities physically based in the United States and, therefore, presumably within the immediate reach of its policing power.[13] (The other three are based in London, Stockholm and Tokyo.) First among equals as regards these operators is, again, VeriSign – which possesses two root server operators.

U.S. control over this crucial function comes to a point in one of these: VeriSign's root server A. Root server A publishes the authoritative root zone file for the entire Internet under a special contract between ICANN's ostensible subsidiary IANA and the Department of Commerce. This contract is legally separate from ICANN's seemingly definitive memorandum of understanding with that same Executive Branch department. In its publicity, VeriSign points up its strategic role by declaring that it "manages…root servers…considered national IT assets by the U.S. Federal government."[14]

Daniel Karrenberg, an expert on the technical features of the DNS, has posed the following rhetorical question: "The majority of the root name server operators are based in the United States of America. Couldn't the US government force them to make any changes it wants?" His answer is unequivocal: "In principle I suppose the U.S. government could do that."[15]

A politically structured distance separates this principle from reality. On one hand, U.S. Executive Branch power over the DNS is not an historical accident but an expression of determined resolve. A defining feature of the domain name system's institutional history is that, in sharp contrast to prior communications systems, no oversight role was allotted to the most democratic agencies of government: Congress and the Federal Communications Commission.[16] Though much-publicized, efforts to devolve the power exercised by the Executive Branch by spinning off ICANN have been nominal, at least thus far. When one founding member of the Internet's technical elite took an abrupt turn in this direction in 1998, a high Clinton Administration official peremptorily declared "that any attempt to manipulate the root without the U.S. government's permission would be prosecuted as a criminal offense."[17] Since then, despite a much-publicized new contract in 2006 which supposedly granted ICANN greater independence from the Department of Commerce, "the root file and presumptive root authority has remained, without exception, in the hands of the U.S. government."[18]

On the other hand, U.S. authorities prefer not to exercise their power over the root. Any overt demonstration of this power would carry far beyond Iran or any other targeted nation. Wholesale curtailment of DNS service with respect to, say, a given ccTLD, and/or a country's top ISPs, commercial and government web sites, and/or its major private networks[19] would likely engender severe "blowback" throughout the entire international community. The result could be to cripple the ongoing effort by ICANN and its sponsors to erect a stable system of governance for the transnational Internet.

ICANN has labored since its inception to build up legally binding contractual arrangements worldwide with state agencies and specialized organizations.[20] Such arrangements are crucial for the smooth functioning of an Internet-based political economy shaped to serve transnational capital. They encompass far more than domain names, extending as well into the oversight and enforcement of property rights in information and the policing of online activity. But this prospective mechanism of Internet governance is as politically sensitive as it is essential. Any U.S. action that might jeopardize its institutionalization, therefore, will not be undertaken without very careful attention to its likely strategic costs.

But let there be no mistake: the Internet's domain name system is largely in the hands of the U.S. Executive Branch and, so far at least, there is little evidence that this power will be voluntarily ceded. At the end of the day, no one but the U.S. administration can say if and when it will be used.

Footnotes

1. Stephen Fidler, "US Demands Europe Bolsters Financial Sanctions on Tehran," *Financial Times* 8 February 2007: 1.

2. National Research Council, Committee on Internet Navigation and the Domain Name System, Computer Science and Telecommunications Board, *Signposts in Cyberspace: The Domain Name System and Internet Navigation*. Prepublication Copy. Washington, D.C.: National Academies Press, 2005: 5-3.
3. There exist other means of disabling Internet access beside those pertaining to the DNS.
4. Milton L. Mueller, *Ruling The Root: Internet governance and the taming of cyberspace*. Cambridge: MIT Press, 2002: 6; see also 216, and Chapter 10, passim.
5. Internet Corporation for Assigned Names and Numbers. *Annual Report 2005-2006*: 6. Retrieved 25 January 2007 at www.icann.org
6. ICANN Annual Report 2005-2006: 19.
7. Muller, *Ruling The Root*: 68; also see Daniel Karrenberg, "DNS Root Name Servers Frequently Asked Questions," ISOC MEMBER BRIEFING #20 January, 2005 Retrieved 12 January 2007 from http://www.isoc.org/briefings/020/
8. For a recent survey of this component of the DNS see LSE Public Policy Group and Enterprise LSE, "A Review of the Generic Names Supporting Organization (GNSO) For The Internet Corporation for Assigned Names and Numbers," Main Report. September 2006: 16. Retrieved 22 January 2007.
9. Milton Mueller and Dale Thompson, "ICANN and INTELSAT: Global Communication Technologies and their Incorporation into International Regimes," Chapter 4 in Sandra Braman, Ed., *The Emergent Global Information Policy Regime*. Houndmills, Basingstoke: Palgrave Macmillan, 2004: 73.
10. Organisation for Economic Co-operation and Development, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, Working Party on Telecommunication and Information Services Policies, "EVOLUTION IN THE MANAGEMENT OF COUNTRY CODE TOP-LEVEL DOMAIN NAMES (ccTLDs)," DSTI/ICCP/TISP(2006)6/FINAL 17-Nov-2006: 13.
11. http://www.verisign.com/verisign-inc/corporate-overview/fact-sheet/index.html consulted 31 January 2007.
12. Milton Mueller, email to author, 20 January 2007.
13. The argument that physical access to portions of the Internet carries with it the feasibility of government control is made systematically by Jack Goldsmith and Timothy Wu, **Who Controls The Internet?** New York: Oxford, 2006.
14. http://www.verisign.com/verisign-inc/corporate-overview/fact-sheet/index.html Retrieved 31 January 2007.
15. Karrenberg, "DNS Root Name Servers Frequently Asked Questions": 14.
16. Mueller and Thompson, "ICANN and INTELSAT": 69-70.
17. Mueller, *Ruling The Root*: 162.
18. Goldsmith and Wu: 146.
19. I follow Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security.* Hoboken: Wiley-Interscience 2006: 365.
20. Hans Klein, "Private Governance for Global Communications: Technology, Contracts, and the Internet," Chapter 9 in Sandra Braman, Ed., *The Emergent Global Information Policy Regime*. Houndmills, Basingstoke: Palgrave Macmillan, 2004: 179-202; OECD, "EVOLUTION IN THE MANAGEMENT OF COUNTRY CODE TOP-LEVEL DOMAIN NAMES (ccTLDs)."