THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

March 2005

Signposts in Cyberspace: The Domain Name System and Internet Navigation—*Summary*

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

Background

The Domain Name System (DNS) enables user-friendly alphanumeric names—domain names—to be assigned to Internet sites. Its distributed hierarchical system of servers, topped by 13 root name servers, converts the domain names into the numerical addresses that the Internet's routers need to locate the sites. Many of these names have gained economic, social, and political value, leading to conflicts over their ownership, especially names containing trademarked terms. As the use of the Internet expanded rapidly in the late Nineties, Congress, in P.L. 105-305, directed the Department of Commerce to request the NRC to perform a study of these issues. When the study was initiated under the sponsorship of both Commerce and the National Science Foundation, steps were already underway to address the resolution of domain name conflicts, but the continued rapid expansion of the use of the Internet had raised a number of additional policy and technical issues. Furthermore, it became clear that the introduction of search engines and other tools for Internet navigation was affecting the DNS. Consequently, the study's task was expanded to include a broad range of policy and technical issues related to the DNS in the more general context of Internet navigation. This report presents the NRC's assessment of the current state and future prospects of the DNS and Internet navigation, and its conclusions and recommendations concerning key technical and policy issues.

Conclusions and Recommendations

DNS. The DNS has performed well through a period of rapid growth, but several technical and institutional challenges must be met for the system to operate effectively as the Internet grows. The system is threatened by malicious attackers, and some governments view control of the DNS as a step towards gaining control of the Internet for broader purposes, such as controlling spam, protecting intellectual property rights, or regulating e-commerce. Administration of the DNS at the highest level should be left to a non-governmental body and not be turned over to an intergovernmental organization.

Currently, the DNS is administered by the Internet Corporation for Assigned Names and Numbers (ICANN) under a memorandum of understanding (MOU) with the U.S. Department of Commerce, which has final approval of ICANN's recommendations and oversees its performance. Commerce will transfer full responsibility to ICANN in 2006 if the organization is able to fulfill a mutually agreed-upon set of tasks. Before the transfer occurs, Commerce should seek ways to protect ICANN from undue commercial and political pressures that may arise in the absence of U.S. government stewardship and to provide for some form of oversight of its performance.

ICANN has been the subject of controversy and contention since its beginning in 1998. Its many diverse constituencies have had concerns about its scope, its processes, and its board. ICANN's perceived legitimacy is more likely to improve by narrowing its scope and improving its processes than by trying to form a board that represents all its constituencies. Though ICANN is charged with administering the highest levels of the DNS, it has varying degrees of authority over three critical elements: the root name server operators, the generic top-level domains, and the country code top-level domains.

The 13 root name servers respond to about 8 billion requests each day for TLD addresses. They are operated by 12 organizations—academic, commercial, governmental, and non-profit—without direct compensation or central oversight. ICANN has no formal agreements with the operators although it is responsible for the stability and security of the system. The combination of diverse autonomous organizations and multiple funding sources has been highly successful and should be continued. A more formal coordination of the operators will be desirable in the longer term, with ICANN currently the best candidate for coordinator. Should one of the operators have to be replaced, ICANN should select the new operator, acting on the recommendations of the other operators.

The 15 gTLDs contain more than 46 million domain name registrations, such as nas.edu or icann.org. Since its founding, ICANN has struggled with whether, when, and how to increase the number of generic top-level domains. It added 7 in 2000 and is currently in the process of selecting up to another 10 for addition in 2005. Adding tens of top-level domains each year for several years would pose minimal technical or operational risk, but the arguments for or against doing so are inconclusive. If it decides to continue adding gTLDs, ICANN should establish a maximum number of top-level domains that can be added annually, set a regular schedule of additions, and consider processes less reliant on staff, board, or expert judgment than those it has used. To protect against severe technical or operational problems, a mechanism should be established to monitor the additions and suspend them if difficulties are identified.

The 243 country code top-level domains (ccTLD), which are associated with specific countries or regions, such as .uk for the United Kingdom, have about 26 million registrations. Currently ICANN has agreements with only a small percentage of them and their participation in ICANN is relatively weak. Since they are such a large segment of the DNS, resolution of ICANN's role vis-à-vis the ccTLDs is one of the critical steps in establishing ICANN's full authority as the administrator and steward of the DNS.

The stability and reliability of the Internet and DNS have depended upon the widespread acceptance of two principles: that the protocols and standards defining their operation would be open and established by the Internet Engineering Task Force (an international voluntary organization) and that innovation in applications would occur at the "edges" of the Internet, rather than through changes in its internal components. ICANN should strengthen its agreements with the operators of the top-level domains to guard against ignoring or misusing agreed Internet standards or practices in order to gain commercial or other advantages. Those operators should inform ICANN in advance of any changes that might have a detrimental effect on Internet or DNS operations or those of other DNS operators. ICANN, in turn, should have an open, transparent, and speedy process of review and approval for proposed changes.

Steps should be taken to improve the security of the DNS: wide deployment of the DNS Security Extension protocols; continued deployment of copies of the root name servers; consideration of the need for further diversification of the location of the Washington, D.C. and Los Angeles clusters of base root name server facilities and personnel; and enhanced monitoring of DNS performance and traffic flows.

The Uniform Domain Name Dispute Resolution Process, which uses arbitration to resolve disputes concerning domain names, has generally been effective and cost-efficient; however, it has weaknesses. ICANN should consider improving consistent use of arbitral precedents, establishing an internal appeals process, using three member panels, improving panelist knowledge about the technology underlying the DNS, and improving the nature and structure of incentives in the process.

Internet Navigation. Internet users face the challenge of navigating through rapidly expanding resources to find the information they are seeking. A range of navigation aids and services have been developed and are being refined to deliver more precise responses to users' searches, in more convenient forms, and to more users. But more development is needed to satisfy the growing needs of more and more diverse users. Among the areas where improvements are needed are: query interfaces and results displays for desktop, portable and collaborative devices; navigation of audio and visual materials; use of contextual information; and understanding of the wide range of navigation behaviors of the highly diverse users who now seek resources on the Internet. Although commercial services can be expected to support development on these topics, academic research has provided the innovative basic technologies for many successful aids and services and support for it should be continued.

A major difficulty with the increased reliance on Internet sources of information is their lack of persistence. Many items once located will not be found at the same location when sought a second time. The providers of information should establish policies that improve persistence; third parties, such as libraries and archives, should act to preserve important Internet resources. Regulatory agencies in the United States and in other countries should pay careful and continuing attention to the ranking of results in response to specified search terms and the display practices of Internet search engines to ensure that they clearly identify those responses that are paid for by advertisers and set them off from those of more neutral searches.

The demonstrated success of the DNS and Internet navigation aids and services in meeting the basic needs of all Internet users should not be jeopardized by efforts to direct their evolution outside of the open architecture of the Internet or to use them to enable control of the flow of information across the Internet.

For additional information:

Copies of, *Signposts in Cyberspace: The Domain Name System and Internet Navigation,* are available from the National Academies Press; call (800) 624-6242 or (202) 334-3314 (in the Washington metropolitan area), or visit the NAP Web site at <http://www.nap.edu/ >.

Support for this project was provided by the U.S. Department of Commerce, the National Science Foundation, and the National Academies. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations or agencies that provide support for CSTB.

COMMITTEE ON INTERNET NAVIGATION AND THE DOMAIN NAME SYSTEM: TECHNICAL ALTERNATIVES AND POLICY IMPLICATIONS

ROGER LEVIEN, Strategy & Innovation Consulting, *Chair;* **S. ROBERT AUSTEIN**, Internet Systems Consortium; **STANLEY M. BESEN**, Charles River Associates; **CHRISTINE L. BORGMAN**, University of California, Los Angeles; **TIMOTHY CASEY**, Fried, Frank, Harris, Shriver and Jacobson; **HUGH DUBBERLY**, Dubberly Design Office; **PATRIK FÄLTSTRÖM**, Cisco Systems; **PER-KRISTIAN HALVORSEN**, Hewlett-Packard Labs; **MARYLEE JENKINS**, Arent Fox Kintner Plotkin & Kahn, PLLC; **JOHN C. KLENSIN**, Independent Consultant; **MILTON L. MUELLER**, Syracuse University; **SHARON NELSON**, Washington State Attorney General's Office; **CRAIG PARTRIDGE**, BBN Technologies; **WILLIAM RADUCHEL**, Ruckus Network; **HAL R. VARIAN**, University of California, Berkeley

Staff

ALAN S. INOUYE, *Study Director;* **CHARLES BROWNSTEIN**, Director; **MARGARET MARSH HUYNH,** Senior Program Assistant; **KRISTEN BATCH**, Research Associate