Monika Ermert and Christopher R. Hughes

What's in a name? China and the domain name system

Book section

WHAT'S IN A NAME? CHINA AND THE DOMAIN NAME SYSTEM (4970 words)

Monika Ermert and Christopher R. Hughes

By taking different political perspectives on China's 'digital leap forward', the chapters in this book assume that there is no such thing as a socially neutral technology. However, while it is evidently true that the social impact of a machine like the Internet depends on the ways in which it is appropriated by particular societies, it is also important to avoid the extreme position of assuming that artifacts can be molded to fit political purposes without any limitations imposed by their technical specifications. The case of Robert Moses the New York builder might demonstrate that a bridge can be used to divide people just as well as it can be made to connect them,[1] yet it is also possible to find examples of technologies that seem to be 'inherently political' in that they demand the formation of certain kinds of political systems if they are going to be used effectively. The classic example is nuclear power, the safe use of which demands a significant sacrifice of civil liberties, through measures such as increasing the use of background security checks and covert surveillance in order to prevent certain materials falling into the hands of terrorists and other criminals.[2]

In the case of ICTs, the Domain Name System (DNS) might be just such an inherently political technology. It is certainly a significant source of political power due to its function of allocating, storing and retrieving Internet addresses. Yet its inherent political characteristics also stem from the degree of centralization that has to be built into the technology if it is to ensure technical standardization and the maximum potential for interconnectivity between systems and avoid making multiple allocations of the same addresses. Whoever exercises control over this

centralized technology, however, inherits the power to decide who exists in cyberspace and under what identity.

Due to the historical development of the Internet, both the central technology and the management system of the DNS has come to reside in the United States. Countries like the PRC, which joined the system relatively late, are thus faced with the problem of trying to establish some kind of control a system that directly affects what they regard to be their rightful portion of cyberspace. By looking at how this situation has come about, this chapter will present the DNS as a case study of how a certain kind of technological development seems to determine certain kinds of decision-making structures, which have in turn led to international tensions between the PRC and the United States.

THE POLITICIZATION OF A TECHNICAL SYSTEM

The technical job of the DNS is to manage the way in which Internet addresses are organized, stored and retrieved. To be efficient, this requires the ability both to allocate addresses according to universally accepted standards and to ensure that such addresses are not duplicated by the many machines that are connected to the Internet for the provision of content and services. Its origins can be traced back to the early 1980s, when Internet administration was still the preserve of a small number of professional computer engineers and standardisation seemed to be no more than a technical and organisational issue to be resolved as the number of computers connected to the Internet rose. Today, this system forms the foundation of the global address mechanism upon which the functioning of the Internet depends.

The basic principles of the DNS were put in place by engineers based in the United States, such as David Mills, Jonathan Postel, Zaw-ming Su and Paul Mockapetris in the early 1980s. They developed the idea of using mnemonic tools as a substitute for unwieldy Internet Protocol (IP) addresses that consist of long strings of digits. An IP address like '123.45.67.891' could thus appear as something like the more meaningful 'www.myuniversity.ac.uk'.[3] By 1985 this priniciple had led to the formation of the DNS standard, which had become widely adopted by 1987.

The need to guarantee interoperability, however, also determined that the DNS should evolve into a centralized system based on an 'A-Root-Server' in which all the TLDs of the official 'root zone' have to be listed. This information is fed to twelve 'slave' root servers on a daily basis. When a request for an address is made, these root servers can then direct the inquirer to the authorized administrator for the relevant TLD. Some of these are private firms like the United States-based VeriSign Inc., which administers '.com' addresses. Others have a closer relationship with government, such as China's CNNIC, which administers '.cn'. Queries then travel to a local DNS server until the information requested is obtained. Such a centralized system thus gives the operators of the A-Root Server considerable power regarding the ability to grant 'existence' and identity in cyberspace, a fact underlined by the shadowy lives of those alternative domain providers who try to circumvent the system.[4]

The DNS is a remarkable achievement when one considers the special kind of 'legislative process' that produced it. The ideas of engineers like Postel and Mockapetris were developed in the form of documents known as 'RFCs', meaning 'Requests for Comment'. Solving technical problems through the circulation of RFCs began as early as 1969, when engineers were

struggling to create common standards to exchange information between what at that time was little more than a handful of computers distributed throughout the United States. Such figures formed themselves into what became known as the Internet Engineering Task Force (IETF), which describes itself as 'unusual in that it exists as a collection of happenings, but is not a corporation and has no board of directors, no members, and no dues'[5]. This informal style of organization and negotiation grew out of the fundamentally libertarian ethos of the engineers involved. This was later to underpin what is known as the 'Open Source' movement, based on the principles that nothing should be kept secret, problems should be solved through collaboration, and all results should be in the public domain.[6] In practice, the RFC process proved to be remarkably efficient, as memos were thus sent out for comment when a technical problem arose, and recommendations were adopted as they gained broad support. Proposals that passed the IETF process were widely respected by the community of developers, who realized the necessity to agree on common standards that could ensure the interoperability of the system.

Great strains were placed on this style of governance by the spectacular growth of the Internet that occurred under the impact of commercialisation in the 1990s, however. The creation of the World Wide Web by Tim Berners Lee in 1991 and the bestowing of authority on the National Science Foundation of the United States by Congress to allow commercial activity on the Internet the following year opened the way for the Internet to become the mass means of communication that we know today. As the number of applications for domain names rose dramatically, the job of allocation that had been handled by Jonathan Postel was contracted out to the private sector company, Network Solutions Inc. (NSI). The allocation of domain names became a profitable activity as NSI was allowed to start charging for its services, and the first 'dot.com' boom saw exorbitant prices being asked for short, easy to recognize addresses like 'www.business.com'.

The United States government further developed its response to the increasingly complex and commercialized nature of the DNS by contracting out its overall management to an organization called the 'Internet Assigned Numbers Authority' (IANA), which was really just the figure of Jonathan Postel himself. Meanwhile, technicians tried to keep up with the rapid growth of demand by frequently updating the RFCs.[7] Several 'Top Level Domains' (TLDs) were introduced, under which individual users could register their addresses. Some of these indicated specific functional constituencies, like '.mil' (for the United States military), '.gov' (for the United States administration), '.edu' (for universities, mainly in the United States), or '.int' (for international organizations). 'Generic Top Level Domains' (gTLDs) were also introduced for more general use, such as the well-known '.com', '.net', '.org', and the more recently introduced '.biz' or '.info'.

Alongside these gTLD's, IANA also created a system of 'country code Top Level Domains' (ccTLD). The names they used were derived from what is known as the 'alpha 2 code elements' used by ISO standard 3166-1. This is the internationally accepted list of all the countries recognized by the UN in abbreviated form (such as 'cn' for 'China'). Going down this route allowed technicians like Postel to avoid interference with politics and getting involved in the sensitive issue of deciding what is and what is not a country. Giving a ccTLD to an entity like Taiwan, for example, could present technicians with a real political problem. However, the use '.tw' has never been opposed by the PRC in the same way that it objects to the island joining international organisations requiring statehood, like the UN. The reason for this could be that according to ISO 3166-1, 'tw' stands for 'Taiwan, province of China'. [8] But it allows Taiwan to

have an ‘independent’ identity on the Internet and the two Chinas to live side-by-side in cyberspace, with their respective managers even having friendly relations.

As the Internet grew in size and complexity under the impact of e-commerce, however, it became increasingly important to ensure that management of the DNS was kept at arms length from interference by the United States government. The solution sought by the Clinton administration was to privatise the service by creating the non-profit-making Internet Corporation for Assigned Names and Numbers (ICANN), which was established under California law in October 1998. From Washington’s perspective, a private corporation seemed like the best way to maintain a centralized system of administration on United States soil that was not under its own control.[9] Yet ICANN has been seen by many as amounting to little more than an oversight body working for the United States Department of Commerce, ensuring the continuation of the American dominance over DNS governance that can be traced back to the early engagement of United States public institutions in the organisation of the Internet.

The technical nature of the DNS makes it hard to see how such a situation can be avoided. The most obvious problem is that ICANN is ultimately subservient to the United States government because the A-Root File is at the heart of the DNS, and any changes to it have to be approved by the Department of Commerce. ICANN thus has to seek approval from the government for any modification, such as creation and changing country zones like ‘.cn’, with all such measures requiring the countersignature of an official of the United States National Telecommunications and Information Association (NTIA), a subdivision of the Department of Commerce.

Concerns have also been raised over the fact that nearly ten out of the thirteen DNS root servers are operated by United States' institutions and companies, the remaining three being in Stockholm, Tokyo and Amsterdam. The fact that United States firms also dominate the market for the provision of domain names is also largely due to the fact that the DNS was developed on American soil. The biggest player is thus VeriSign, which acquired NSI in 2000 and which is also contracted by ICANN to manage the A-Root Server on its behalf, under supervision by the Department of Commerce. Finally, the fact that ICANN is established as a Californian corporation raises the issue of whether the registrar companies which it accredits to administer domain names around the world, come under United States jurisdiction.

Such developments have led many critics of ICANN to conclude that there needs to be more international participation in the decision-making process, especially concerning initiatives such as the selection of new gTLDs, like '.info' and '.biz'. Yet moves to 'democratize' ICANN have so far proven to be rather farcical. As a private corporation, it is governed by nineteen directors. An attempt to make this board more democratic was made when nine of these positions were made into 'at large' representatives of five 'world regions', and were elected by on-line ballot in October 2000. The winner of the 'at large' directorship to represent all Internet users in the Middle East, Pakistan, India, China, Japan, Australia, Afghanistan and 'countries to the East', including the East Indian Ocean islands and Antarctica, (but excluding United States and Latin American possessions) was the Maryland-based Japanese employee of Fujitsu, Masanobu Katoh, who polled no less than 13,913 votes!

An attempt to satisfy the demands of states to have an input into the decision-making process was made by creating a General Advisory Committee (GAC), which consists of representatives from

32 concerned national governments, including the PRC. This body has issued principles which attempt to reassert the authority of states, by requiring that any domain name registrar should only be approved by ICANN after a communication has been received from the host government to authorise its existence, and that if an administrator does not have the support of the local community and authorities then its license should be reallocated to another delegee. Ultimately, however, the concentration of power that is decided by the technical nature of the DNS means that there are can be no binding force to make such changes to the management system of ICANN effective in achieving a more representative system of governance.

The answer is thus sought by some critics of ICANN in the development of a more decentralized technical system. In Europe, for example, discussions are going on about the development of a parallel root server system.[10] In Asia, one of the most outspoken advocates of a decentralized method for overseeing DNS administration is Tan Tin Wee, Associate Professor of Biochemistry at the University of Singapore.[11] Tan is chairman of the Multilingual Internet Names Consortium (MINC) which has gone beyond Asia to find partners in the Arab and African worlds. Several of his students were also prime movers in the establishment of iDNS.net, a spin-off enterprise of the University of Singapore that carries out research on Chinese domain names and has become a key pressure group in the growing movement for the internationalization of the DNS.

CHINA ENTERS THE DNS

China itself entered the DNS at a comparatively late stage. The first network link between China and the outside world was established on 20 September 1987 when the Chinese Academic Network (CANET) was connected to the Internet through cooperation between the Institute of

Computer Application (ICA) in Beijing and the University of Karlsruhe.[12] It was not until 1990, however, that the ccTLD '.cn' was delegated by Jonathan Postel to Professor Qian Tianbai, then deputy chief engineer at ICA and manager and administrator of the CANET. In 1993 CASNet, operated by the Chinese Academy of Sciences, began to study the DNS, and the following year Qian Tianbai started to actively manage the '.cn' space for China, again with assistance from the University of Karlsruhe. It was not until 1994, though, that China's first Website, 'Window on China', went online.

According to CNNIC's account of this process, one of the reasons for China's late entry into the system was that the National Science Foundation of the United States rebutted requests for an 'official' connection to the Internet several times during 1992 and 1993. This, claims the CNNIC, was because Washington opposed any socialist countries gaining access to the Internet, due to the amount of scientific and technological information it contained and the number of its own official institutions that had already gone on-line. [13] From the American perspective, however, the delay was due largely to the fact that the Chinese had not yet gained a proper understanding of how the Internet works. Cindy Zheng of the San Diego Super Computer explained after a visit to China in 1993, for example, that while the United States did impose restrictions on the export of high-end computer systems to China, additional difficulties were created for joining the DNS by other factors. For example, the Chinese did not realize that they should approach commercial carriers and network providers for a positive response to their requests, rather than government officials. The way in which networking projects in China were jointly funded by the World Bank and the Chinese government also caused problems. Of special importance, though, was the high degree of distrust that existed between the different institutions taking part in the National Computer

Networking Facility of China, which brought together the main academic research institutions involved in computer sciences.[14]

Such distrust between Chinese institutions may have partly been due to the general situation that existed before computer networking began to be regulated in the mid-1990s. As in other countries, academia had been the original driving forces behind the Internet in China, but funding had been sparse and partly derived from foreign research institutions. When the need for coordination grew with the rising number of institutions setting up their own networks and links to the outside world, there were no existing models for cooperation, and ICANN's practice of consensus-based self-regulation was viewed with suspicion. As the 1994 INET-Report on Networking in China makes clear,[15] the result was a situation in which too many ministries and other authorities were involved in decision (or non-decision) making. These included the State Science and Technology Commission, the Ministry of Posts and Telecommunications, the Ministry of Education, the Ministry of Electronic Industries, the Beijing Posts and Telecommunications Administration, and other regional and provincial authorities. According to the INET-Report, there was no agreement among these bodies about the importance of academic networking and how to pay for the development and operations of the various networks.

Such a situation may well have been a primary reason for the slow progress of the setting up of the '.cn' DNS registry. In this situation of bureaucratic competition, no agreement could be reached on who should be in charge of the assignment and management of domain names, and how the domain name server should be set up and managed. As Cindy Zheng points out, different opinions arose over issues such as whether the naming system under '.cn' should be organized according to a geographical substructure, or with second-level generic domains according to the

existing gTLD-scheme, such as '.com.cn', '.org.cn'. The settlement of such disputes had to wait until a regulatory system had been established and a degree of centralized authority had been created in the form of the CNNIC, a non-profit organization wholly owned by the state, and controlled by the Informatization Group of the State Council.

The establishment of the CNNIC, however, meant that domain name registration had effectively become a function of the Chinese state. Although there are no clear rules by which the organisation maintains the 'purity' of the various second-level domains, it claims the right to administer not only the Chinese namespace under the ccTLD '.cn', but also to require notification from operators of servers in China using any other domain. Domain registrants have to be institutions or companies, and not individuals, while foreigners have to have residential status. All have to be able to produce a document of verification from the organization for which they work. The CNNIC is also unique in the world for the way in which it carries out a manual check of applicants' documents. The workload as a result of that procedure may provide some explanation for the comparably high annual registration fee of RMB 300 per domain that is set by CNNIC's.

Although it is hard to assess just how many of the CNNIC provisions are effectively executed, the Chinese authorities have at least established the principle that it is they who have the right to maintain a tight grip on what they consider to be their rightful namespace. The state has also expanded its control over the CNNIC structure through a number of measures that reduce the input from academics. When the CNNIC was established, for example, the research institutions that had previously been engaged in DNS administration were absorbed into a kind of oversight body, known as the 'Steering Group', which meant that the Chinese Academy of Science (CAS)

lost its direct influence over day-to-day management. This movement away from academic involvement continued when the MII was established and took over the job of supervising the CNNIC from the Informatization Group of the State Council. Under the new MII regime. Moreover, the CNNIC Steering Committee was reorganized to bring in commercial telecom players, like China Telecom, as associate members.

Despite the bureaucratic politics surrounding management of the DNS in China, however, the number of domains registered has grown dramatically as uptake of the Internet has increased. While there were only two hosts in the '.cn' domain two years after its management was delegated to Qian Tianbai in 1990, and around 1000 before the establishment of the CNNIC, by the end of 1997 the number had risen to 5000. Today the figure has reached 127,319. The majority of those that come under the '.cn' domain are registered as '.com.cn', which means that they are commercial organizations (see Chart 2.4). However, Chinese users can also register under the gTLD '.com', which makes the ccTLD '.cn' redundant. It is impossible to put a figure on how many users do this, but there are certainly registrars who sell '.com' domains in China at a cheaper price than '.com.cn'. It is worth noting, moreover, that there is no official figure for the number of foreign companies that have registered under '.cn' either.

THE CLASH OF SYSTEMS

With both the United States and the Chinese governments attempting to exert control over an increasingly commercialized DNS, it was inevitable that frictions would arise between them. This was especially so when ICANN decisions began to have a direct impact on the nascent market for selling domain names in China when the first 'dot.com' boom took off in major cities. Indigenous

telecommunications providers, such as the Zhejiang-based Eastern Communications Co., (Eastcom), had in fact been quick to make efforts to enter the international market as operators of new gTLDs, well before other Chinese firms began to prepare for WTO accession. As part of the strategy to gain a share of the market, Eastcom successfully applied to become an ICANN accredited domain name registrar.

Eastcom quickly came under pressure from the United States, however, when a Virginia court ruled that the Hong Kong and Shanghai based company Maya should relinquish the domain name 'CNNews.com' to AOL-Time Warner-Subsidiary CNN. Maya, however, had registered its claim to the CNN domain name with Eastcom. ICANN's legal counsel and vice president, Louis Touton, ordered Eastcom to comply with the ruling by the United States court. According to the court protocols, the judge also considered ordering VeriSign/NSI, the central '.com' registry, to cancel the domain registration lodged by Eastcom. Although he explained that the court had no power to order anybody in China to do anything, he also reasoned that it had jurisdiction over the NSI.[16] The implication of this threat to impose a cancellation order on VeriSign/NSI, or on a non-United States based Registrar like Eastcom, is that anybody registering a domain name comes under United States jurisdiction, regardless of whether they go through a Chinese, German or South African ICANN accredited registrar.[17] Not surprisingly, the dispute over 'CNNews.com' led Maya to warn the Americans,'Yankee, don't bully people too much'.[18] Such sentiments resonated well with general criticisms in the Chinese press of what are seen as the ambitions of the United States to exert its hegemony in cyberspace.

Further frictions between the United States and China have also been created over the introduction of standards for the use of Chinese-language domain names. This problem arises

because the DNS was originally limited to using the American Standard Code for Information Interchange (ASCII), which consists of the Roman alphabet and a number of graphic symbols. While most western countries are satisfied with this choice, even though they are denied the use of national language characters like the German umlaute and French accents, the call for nationalized versions of domain names has grown in many Asian and Arabic countries. The first trials of Chinese domain names were started in the late 1990s by Singapore's 'iDNS.net', as Tan Tin Wee argued that a reform of the DNS had to follow on the sinicization of software and e-mail and pushed for rapid movement towards the adoption of an internationalized system.[19]

In China itself, the CNNIC began to conduct research on developing domain names using Chinese characters in 1998 and in January 2000 it started to carry out tests using software that could impose a Chinese character address on top of an English address. This project expanded to take in the 'four territories and two coasts' (Mainland China, Hong Kong, Macao, Taiwan) when a Chinese Domain Name Consortium was established on 19 May 2000. Complaining that using English addresses on the Internet is like using an English-language map in a Chinese city, participants in this venture were particularly concerned that being forced to use English addresses for e-commerce would impose real disadvantages on established Chinese brand names.[20] Yet such a movement provoked concerns at ICANN, despite assurances that the new consortium would meet international standards by working with international organisations.

It is in this context of growing international frictions that the American firm VeriSign was accused of 'infringing on China's sovereignty'[21] when it started to create its own technical standards for Chinese domain names. In the autumn of 2000 VeriSign announced that it would start registering Non-Ascii domains, including Chinese, first on a trial basis and using a technical

standard that they thought would be the most viable within the ongoing discussion in the IETF.[22] The CNNIC reacted quickly by demanding a stop to VeriSign's activities. Its director, Ma Wei, explaining to a press conference in Hong Kong that 'We hope that Chinese people would have the mandate over Chinese domain names'.[23] However, its main argument against VeriSign's initiative was more sophisticated, and relied on complaining about the fact that no international agreement had yet been reached on a common technical standard for Chinese names, so the IETF and ICANN should put pressure on operators to wait until global compatibility could be ensured. The Chinese representative in ICANN's GAC thus urged the board of directors to stop VeriSign from leaving its test-bed environment and moving towards full-scale registration of Chinese domains. The GAC responded to such pressures by issuing a communiqué listing nine principles to constrain operators from leaving their testbeds without first gaining the general consent and coordination of a community-based framework such as ICANN. [24]

When ICANN proved reluctant to stop VeriSign grabbing another part of what CNNIC and Chinese operators regarded to be their rightful market, the result was further alienation from the American-centred Internet governance system and even greater skepticism towards the process of bottom-up standardization. Chinese officials have criticized initiatives such as those taken by Verisign for being a kind of linguistic hegemony. As Minister for Information Industry Wu Jichuan put it to the Pacific Telecommunications Conference, 'Due to historical and technical reasons, 90 per cent of the information available on the Internet is in English and the overwhelming majority of it is generated from developed countries, whereas developing countries are mostly information receivers. As information flows across borders and developing countries are absorbing advanced technological and cultural information, their cultural traditions, moral standards and values have been severely challenged.'[25] An organization like CNNIC thus

sees sinicization of the DNS to be one of its main goals in a battle to prevent American technological and cultural dominance of the Internet.

CONCLUSION

Bearing in mind the common perception that the Internet is a technology that erodes the power of the state, it is somewhat ironic that one consequence of the informal development of a technically centralized DNS structure has been the concentration of administrative power in the United States. The above account has shown how this situation has created political tensions between states as governments around the world have tried to exert their influence over what has become a central institution of Internet governance. China has been a party to such disputes partly because it joined the DNS relatively late and then felt it necessary to take measures to regain control over the address system where it had a direct impact on its commercial activities. Domestically, this meant the state winning control from the academics and engineers who were originally entrusted to run the system. Internationally, it required responses to measures taken by the United States government that appeared to consolidate the centralization of decision-making power under American jurisdiction.

A further twist in the story appears with the corresponding growth of opinion in bodies like ICANN's GAC that domain name registration should now be recognized as an official function of states. Within China, the government has taken its own measures to challenge the technological status quo by putting in place bureaucratic and regulatory structures to exert control over its ccTLD. While China is lobbying for acceptance of this model by the international community, however, it can do little about the fact that the technical structure of the DNS

concentrates real power in the A-Root Server, which is located on American soil and is ultimately under the control of the United States Department of Commerce. Moreover, the technological capabilities of American corporations like VeriSign, means that even indigenous Chinese attempts to define standards for a Chinese-language name system are being challenged from across the Pacific. The DNS, as it has developed so far, therefore, appears to be an inherently political technology that determines the formation of a centralized power structure. Any movement away from this will depend as much on the development of new standards and architecture as it will on the ability of states to put in place a more satisfactory system of global governance.

---

[1] R.A. Caro, *The Power Broker: Robert Moses and the Fall of New York*, (New York: Random House, 1974). See also L. Winner, 'Do Artifacts Have Politics?' in D. Mackenzie and J. Wajcman, *The Social Shaping of Technology* (Second Edition), Buckingham and Philadelphia: Open University Press, 1999, p. 30.

[2] L. Winner, 'Do artifacts have politics?', pp. 33-8.

3 T. Denton, 'The Governance of the Domain Name System'. Online. Available HTTP: <http://www.tmdenton.com/Speeches/The%20Governance%20of%20the%20Domain%20Name%20System.htm> (accessed 5 April 2002).

[4] There are several alternative TLD-operators, such as Image Online Design or the various organizations that are grouped under the Open Root Server Confederation (ORSC). None of these, however, is able to attract large numbers of ordinary Internet users.

[5] IETF, 'The Tao of the IETF: A Novice's Guide (RFC 3160)'. Online. Available HTTP: http://www.ietf.org/tao.html#intro (accessed 21 May 2002).

[6] On the RFC process see John Naughton, *A Brief History of the Future: The Origins of the Internet*, London: Weidenfeld and Nicolson, 1999, pp. 137-9.

7 Most notable are RFC 1034 and RFC 1035, written by Mockapetris, which superseded earlier drafts. Details of DNS-related RFCs can be found on the IANA Website. Online. Available HTTP: <http://www.iana.org> (accessed 1 June 2002).

[8] For the full list of the alpha-code-2-elements of ISO 3166-1 see 'English Country Names and Code Elements'. Online. Available HTTP: <http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html> (accessed 21 May 2002).

[9] United States Department of Commerce, 'Management of Internet Names and Addresses'. Online. Available HTTP: <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm> (accessed 1 June 2002).

[10] Andy Mueller-Maguhn, 'elected' as the so called ICANN 'at-large Director' for Europe has put an independent European root zone on the ICANN agenda several times.

[11] See proceedings of the ITU-conference on Multilingual Domains, especially Tan Tin Wee, 'Policy and Coordination Issues in Multilingual Internet Names'. Online. Available HTTP: http://www.itu.int/mdns/presentations/dayone/tan1.ppt (accessed 30 May 2002).

12 CNNIC, 'Evolution of the Internet in China'. Online. Available HTTP: <http://www.cnnic.net.cn/evolution.shtml> (accessed 9 April 2002); B. McIntyre, 'China's use of the Internet', in P. Lee (ed.), *Telecommunications and Development in China*, New Jersey: Cresskill, 1997, pp. 159 –169.

[13] CNNIC, 'Evolution of the Internet in China'.

14 Cindy Zheng: A Special Report - Current Computing/Networking Status in China, China News Digest, Special Issue on Networking in China, 11 July 1993. Online. Available HTTP: <http://www.sdsc.edu/~zhengc/93trip.html> (accessed 12 May 2002).

15 F. Kuo, J. Ding, C. Zheng, F. Hussain, *Issues in Academic Networking in the PRC: INET 1994 Report*, San Diego Supercomputer Centre Website. Online. Available HTTP: http://www.sdsc.edu/~zhengc/inet94.html (accessed 30 June 2002).

[16] Court protocol available online. Available HTTP: <http://www.cptech.org/ecom/jurisdiction/CNNEWS.pdf> (accessed 1 June 2002); <http://www.cnnews.com/topic/388.shtml> (accessed 1 June 2002).

17 In addition to '.com', the registries for many other gTLDs are also located in the United States. For example, Verisign also has the official registry for '.net', '.org' and '.edu'. The registries for the two newest gTLDs, '.biz' and '.info', both have offices in the U.S. in addition to Australia and Ireland. Thus, under the Virginia court's interpretation of the ACPA, every domain name that is registered under '.com' or any of the other above-mentioned gTLDs, is subject to U.S. jurisdiction. See V. Polak, W. Matus and S. Gelin, '".com" Domain Names can Lead to U.S. Jurisdiction', *Internet Law Journal*, 2 February 2002. Online. Available HTTP: <http://www.tilj.com/content/litigationarticle01300201.htm> (accessed 10 April 2002).

[18] Cnnews.com, 'Meiguo lao, bu yao qi ren tai shen', 12 April 2001. Online. Available HTTP: <http://www.cnnews.com/maya/cnnews/zt/ztwz/item/2001_04/486780.shtml> (accessed 1 June 2002).

[19] International Telecommunication Union, 'Joint ITU/WPO Symposium: Creating a wider understanding of the complex issues surrounding the implementation of multilingual domain names', 22 February 2002. Online. Available HTTP: <http://www.itu.int/itunews/issue/2002/01/joint.html> (accessed 31 May 2002).

[20] CNNIC, 'CNNIC tuichu zhongwen yuming shiyan xitong' ('CNNIC Promotes Experimental Chinese-Llanguage DNS'). Online. Available HTTP: <http://www.cnnic.net.cn/cdns/about_cdns.shtml> (accessed 1 June 2002).

[21] Reuters, 'China Claims Its Own Domain'. Online. Available HTTP: <http://www.wired.com/news/politics/0,1283,40506,00.html> (accessed 1 June 2002).

[22] For details on the testbed see VeriSign, *General Information Paper on Internationalized Domain Name Resolution*, 3 April 2001. Online. Available HTTP: < http://www.verisign-grs.com/idn/Gen_Info_Paper.pdf> (acccessed 31 May 2002).

[23] Reuters, 'China Claims Its Own Domain'.

[24] ICANN, 'Communique of the Governmental Advisory Committee, March 10, 2001', and 'Communique of the General Advisory Committee, June, 3rd 2001'. Online. Available HTTP: <http://www.icann.org/committees/gac/communique-10mar01.htm> (accessed 1 June 2002); <http://www.icann.org/committees/gac/communique-03jun01.htm#Attachment> (accessed 1 June 2002).

[25] Roman Rollnick: China concerned at electronic threats to moral standards. Earth Times News Service, 14 January 2002. Online. Available HTTP: http://www.earthtimes.org/jan/telecommunicationchinajan14_02.htm. For a discussion of security issues stemming from dependence on international networks see article by Christopher R. Hughes in this volume.