Internet Governance, National Interest and International Relations

Background Paper for the
United Nations ICT Task Force Meeting
24-26 March 2004, in New York

By Kenneth Neil Cukier
Research Fellow, National Center for Digital Government
John F. Kennedy School of Government, Harvard University

Six long words. Three big concepts. One small idea. The title of this essay comprises things not normally associated together.

When one considers the Internet and foreign affairs, it is usually viewed in terms of cross-border regulations on content and usage, or the effect of the medium abroad (for example, regarding "soft power"), or the change in the process of diplomacy itself.

However, there is another dimension, which is the focus of this essay: who controls the network's operation and evolution? This is currently done by ICANN, the Internet Corporation for Assigned Names and Numbers. It was created by the US in 1998 as an international, public/private-sector body to oversee the Internet's domain name system – a task previously managed by the US Defense Dept., which initially funded the Internet.

The one simple idea is this: *The Internet is a global resource whose control and allocation is a matter of political power; instead of doing away with geopolitics, the Net creates new areas of national interest and foreign policy concerns.*

This essay doesn't presume to offer a doctrine for foreign policy in the Internet age. Its more modest goal is to raise a number of empirical matters that governments collectively face regarding the network. Together, they reveal a new and mature way of understanding the medium.

The first part explains Internet governance, or "infrastructural coordination." Part two looks at it from the perspective of national interest, with an emphasis on US interests. Part three notes how these interests map to specific ICANN issues, which are concerns of international relations. The fourth part tries to explain why ICANN matters not just for students of politics and international affairs, but for ordinary individuals, companies and other stakeholders. Finally, the essay concludes by analyzing current tensions concerning the Internet's institutionalization.

I. Internet governance

It is a regrettably misleading term (since "governance" sometimes presumes it is the sole responsibility of governments). A better term may be "coordination of Internet technical functions" though they may present public policy concerns, too. There are four aspects:

- **Names** (global ones like .com; territorial ones like .iq for Iraq). Who says who is a registry, a valuable economic asset that effects free speech? Who says who gets a country-code, an important way to establish presence online, and symbolically important?

- **IP numbers** (e.g. "255.255.255.0"). A valuable and finite resource that affects the types and number of devices that can connect seamlessly to the network. When the network was young, huge blocks of numbers were given to US companies and universities, so some benefit from abundance while entities outside the US deal with relative scarcity.

- **Protocols** (TCP/IP, SNMP, etc.). Most communications standards have been set by national and intergovernmental bodies; the Internet's standards exist outside that process, which has historically led to tension with the ITU, among others.

- **Root servers** (1 master, 12 slaves, +30 mirrors). The computers match domains to their authoritative name servers for routing traffic. Currently, three are outside the US (Sweden, UK and Japan); the majority are under US governmental control. Mirror servers have been broadly diffused globally, providing advantages in routing, but meaningless in terms of internationalized political control.

These function sound technical and arcane – and they are. That's one reason why many countries have been late to understand their geopolitical importance. Control over these aspects of the Internet is akin to a central bank's control over a nation's money supply. Names are the real estate of the Internet; numbers are the oxygen or oil of the network; the protocols are the utilities, or the legal system (from which the term intentionally derives); root servers are the central nervous system. Together, the system is important, and its daily operation as well as the influence over the substance of policy and institutional process represents important power in the modern age.

II. National interests related to Internet control

The question of what constitutes a national interest is a long-standing debate among scholars; this essay won't go there. Nor, try to separate vital from secondary interests; that's for another time. Instead, it is meant for identification, not prioritization.

A few interests, along with where they fit in with the ICANN-related functions, include:
- Access to numbering resources (IP address space).
- Stability and robustness of network (root servers and protocols).
- Access to improved media resources (domain names and content).
- Greater economic efficiency via new technology (protocol development).

These interests aren't universal; in fact, in some cases they may conflict with interests of certain nations, for instance:
- An authoritarian regime would prefer a closed medium to control information flows.
- Greater technical efficiency may jeopardize the revenue of existing state-run firms.

But the interests correspond to objectives the Internet can support and fuel:
- Economic development.
- Openness, transparency, accountability.
- Free expression and information sharing.
- Continuing technical innovation.
- Global political, economic and social stability.

Of course there is nothing about the Internet that inherently supports these goals – it must be shepherded in the right way. But the Internet, as a more open medium compared to all other communications technologies, can potentially further these goals by dint of its end-to-end design principle. This provides for its decentralization, lower cost, and openness.

III. How Internet governance interests dovetail with foreign affairs

There are pragmatic concerns facing Internet governance and nation-states, that have escalated to the level of international relations. They include:
- National sovereignty over information infrastructure
- Control over shared information resources
- Influence over policy process and substance
- Access to content and its restriction

Each of these areas contain practical policy concerns, and merit closer consideration.

National sovereignty over information infrastructure:

- *ccTLDs: Who is a country?* – ICANN and its predecessor organization, has always sought to avoid the issue of what is a state, yet is inherently unable to skirt it. For instance, in 2003 Chinese authorities raised the issue with US and ICANN officials of why .tw existed since it seemed to legitimize the island as an independent nation, which China regards as a province. Though China stopped short of asking its removal (there are a number of non-national territories in the ISO 3166 list, including .hk for Hong Kong), the incident is indicative of the offline politics that can easily enter domain name policy discussions. Secondly, in March 2000, ICANN established .ps to represent the Palestinian Authority, another example of how politics is implicit in Internet addressing.

- *ccTLDs: Who controls the domain?* – There is a policy ambiguity over who has ultimate authority over county-codes. In 2003, Singapore's governmental country-code registry withdrew its application for a trademark on its two-letter domain, .sg, after ICANN informed it that the country didn't actually have rights to the domain; instead, ICANN controlled it. Rather than force the issue, the government acquiesced. The incident exposes the ambiguity of whether countries have sovereignty of their country-codes, and why ICANN asserts it ultimately does when the US government's 1998 statement of policy (White Paper) that established ICANN's principles indicated the contrary. At the UN World Summit on the Information Society in Dec. 2003 in Geneva, Zimbabwe's President Robert Mugabe emphatically called this an example of neo-colonialism.

Control over shared information resources:

- *International domain names* – IDNs are a nascent technology that permits domain names in languages other that don't use the Roman alphabet characters; it opens up Internet addressing to all the world's scripts. However, unlike country-codes where there is normally one acknowledged entity that represents the nation, major languages often transcend one specific country, such as Arabic or Chinese. China initially claimed sovereignty over the language for the domain name system; it has since relinquished the stance. But the question of who decides what entity is legitimate to steward and set policies over a script is uncertain. Because the values and traditions of the speakers vary widely across cultures that share a language, the entity designated to register names can affect the degree of free speech or privacy online.

- *Internet Protocol numbers* – The addresses represent important economic value and their access is vital for widespread deployment of Internet-enables devices. Japan's consumer electronics industry is dependent on access to IP addresses; in 2001, the country's minister of industry traveled 40 hours roundtrip for a three-hour visit to an ICANN board meeting in California, to make that point. China relies on access to IP addresses due to its huge population; for that reason it specifically obtained an unprecedented two seats on executive council of APNIC, the regional Asia-Pacific IP number registry, so it has greater influence over the allocation process. Lastly, global mobile phone companies or handset makers will depend on access to IP numbers. These allocation concerns will remain despite an upcoming enhancement called IPv6, which increases the number of addresses exponentially.

- *Root servers* – The constellation of 12 secondary root servers, capped at that number due to technical limitations, are managed by both private and public entities that are only loosely affiliated with ICANN, for historical reasons. Many countries have requested to operate a root server, including France and China. Global deployment is important for better regional traffic routing and quality of service, for network resiliency, for symbolism of internationalized Internet control and national prestige. It could potentially prevent any one entity from having a preponderance of control to unilaterally affect the addressing content that the rest of the Internet adheres to for universal interoperability. The use of mirror servers have led to better regional traffic routing, but confers no political control, and lacks the symbolic power that control infers.

Influence over policy process and substance:

- *Process* – The central intergovernmental debate at ICANN is over the role of the state versus private stakeholders, such as industry, technologists or civil society. ICANN's Governmental Advisory Committee has no formal policy-making powers, which some member states feel is inappropriate. ICANN itself is a creation of the US government and lacks the formal legitimacy that international treaties confer. Moreover, the GAC exhibits classic politicization of offline disputes, such as when China walked out of a meeting in Melbourne in March 2001 when it saw "Taiwan" name cards for the island's representatives, rather than the traditional diplomatic word-play "Chinese Taipei."

- *Policy* – ICANN has set policy in a few areas, either by action or non-action, that impact national law. For instance, one of the first acts the organization took was to establish a uniform dispute resolution procedure (UDRP) for generic, global domain names. This was a method of enforcing trademark rights globally, by adopting the procedure developed by WIPO. Secondly, ICANN has not changed the public nature of the WHOIS database for global domains, which makes openly available the name, address and phone number of registrants. It has been roundly criticized for violating norms of privacy. The reason it remains public is due to the influence of intellectual property holders who insist on having an easy way to contact Web site owners in cases of infringing content. These two examples underscore how the substance of ICANN decisions, by act or inaction, affect national policy matters and apply globally.

Access to content and its restriction

- *Protocol* – The way the technical code of the Internet works makes identifying, tracing and monitoring traffic difficult. There is also an inherent tradeoff between security that protects the integrity and confidentiality of communications needed for e-commerce with the potential for surveillance capability needed by law enforcement. In 1999, the US Dept. of Justice sought to develop wiretap capabilities directly into the protocol of the Internet, via the standards body IETF, which is affiliated with ICANN. The initiative was rebuffed by the technical engineers, but underscores an area where national interests coincide with how the Internet operates, that matter for international relations.

These areas are of course not exhaustive. And the examples used are often just ones that stand for a number of similar incidents. Lastly, one of the most important aspects of the Internet relative to governments is network security, but this analysis has not included it as a point because, so far, there has not been a political dispute in that regard.

IV. Why ICANN matters

ICANN's actions affect how people use the Internet on a daily level. It does so because of its control over names, numbers, protocols and the root server system that holds it together. However, due to the idiosyncratic ways that the Internet evolved (informally, often non-governmentally, inherently internationally, etc.) its institutional structure remains largely outside the realm of classic national and intergovernmental control. Any entity that strives to "govern the Internet" in terms of the quasi-technical related functions will posses significant power, but also confront contentious issues.

Names.
- The power to decide the words that everyone in the world will use to communicate, identify content and interact online. This responsibility over the upper-most hierarchical terms is crucial for helping users navigate and give semantic meaning to the online world.
- That lets the institution delegate an enormous economic and political asset to an entity, to operate the domain registry.

- The delegation permits it to influence the policies that the registry must follow concerning the appropriate use of words for domain names, which directly impacts freedom of speech and democratic dissent. It also determines the degree to which trademark holders are protected.
- Oversight of registry operations and as a result, the WHOIS database, gives it control over the degree to which privacy and anonymity exist at the most primal aspect of Internet communications – online identity, and entry-point of access.
- Authority over the system lets it regulate the companies that sell domains, to ensure fair competition, consumer protection, and to a certain degree, the prices users pay.
- This power effects the visibility of individuals and companies on the Internet.

Numbers.
- The control of IP number assignments effects the way the Internet evolves in terms of its growth, cost, future services and openness to technical innovation.
- Power to determine address allocations impacts the number of devices that can connect directly to the Internet, which affects how many people or machines are online.
- The policies determine the cost of IP addresses (one-time or annually-recurring fee), and effects the price that consumer and businesses pay to go online, as well as the economic model of businesses that rely on the deployment of network infrastructure.
- Power to control access to IP numbers impacts the types of services users are offered, by affecting a company's ability to bring onto the network millions of devices or objects via embedded addresses.
- Oversight of allocations can be used as a mechanism to achieve non-technical, policy goals, such as, if implemented, positively identifying users and their precise geographic location, for activities like surveillance, taxation, etc.
- Controlling address availability impacts the openness of the Internet as a medium for technical innovation, by ensuring widespread address distribution so that devices can connect directly to other devices without the need for intermediaries that could act as a choke-point for network control. (Such control could entail prohibiting applications like Internet telephony or peer-to-peer file sharing, etc.).
- Power over the network's openness assures the degree of user independence relative to the Internet service provider, that enables competition and usually lowers costs.
- The ability to preserve network openness affects democratic values of free expression; control of IP addresses could otherwise provide power over who may participate online.

Protocols.
- Control over the development of new protocols effects the degree of technical innovation that can happen online, and what users are able to do.
- New protocols can be a means to remedy problems with the current design and operation of the network, such as devising service quality systems.
- That power over can translate into control over code development to achieve mainstream policy-related objectives, such as privacy, censorship, surveillance, etc.
- This control could also be used to prohibit certain activities such as content restrictions, or hobbling functional capabilities of the network, like file-sharing.

Root server system.
- Oversight authority ensures the stability and smooth functioning of the critical infrastructure of the Internet, so that traffic is routed efficiently and accurately, leading to quality of service for users and confidence in the network for new and sophisticated uses.
- Geographic distribution of root servers provides more efficient traffic routing (of address queries), which lowers cost and increases quality of network performance.
- This decentralized distribution, if coupled with control of the server, can risk a fragmented addressing system, if the entity decides to change any of the content in the zone file (adding or deleting a name, or changing the authoritative name server address).
- Contrary-wise, decentralized distribution can act as an insurance policy to assure that no single actor holds so much control that it can unilaterally change the zone file in a way that other root operators have an incentive to unwillingly follow to prevent fragmenting the addressing system.
- Control of a root server could be used for surveillance (albeit extremely inefficient) of Internet traffic connections (though not content).

Final Thoughts: Institutions and Governance

This analysis points to a paradox of Internet governance. It might framed as the paradox of power and plausibility: the more horrific the scenarios of how Internet governance can be potentially abused, the less likely it will actually happen.

This should provide some relief. It injects a dose of reasonability and proportion to the debate, since it isn't always big, abstract principles and hypothetical scenarios one considers, but practical questions of how to implement concrete policies in the real world.

Still, there are some fundamental tensions regarding the institutionalization of Internet governance. It is essential to balance:
- the need for openness with specialized expertise;
- representation with the naturally unequal influence of diverse stakeholders (and ability to continually add new ones);
- the application of the rule of law with the risk of politicization;
- established processes with flexible implementation for new circumstances;
- stability with experimentation to preserve continued innovation.

If there is an underlying conflict that drives the debate, it may be the question: "What is the Internet?" It is not a metaphysical concern, for the answer one gives effects whether one regulates / controls / manages / coordinates / oversees / ignores the medium. Questions about what constitutes the Internet include:
- Global public resource or common private good?
- Innovation at the core or at the edge?
- Commercialization of infrastructure or at higher layers?

Ultimately, we can hope there's more Internet governance or less of it; we can strive to centralize or decentralize the processes – and it seems appropriate to initiate a global discussion with ever-increasing numbers of stakeholders on these matters. But that is provided we are willing to do the harder work of agreeing on answers.

Conclusion

After having examined the specifics of Internet governance, it may be useful to return to the bigger picture – and the "one small idea" with which I began this essay. If a hands-off approach or watching (and, hopefully, learning) from the sidelines was an acceptable policy for governments in the 1990s, it clearly isn't an option anymore. The Internet has become too important for governments to remain passive observers to its development, and the issues, this essay has sought to argue, has become an urgent matter of national interest, power, security and sovereignty. And thus, a matter of foreign policy.

As such, there are two extreme directions in which governments may go:
- Deviating in some way from the ICANN-sanctioned naming and numbering system.
- Becoming excessively engaged, seduced by ICANN's true or perceived power.

On the former, why one ought care if a country decides to drop out of the ICANN addressing system is strait-forward: the value of a network decreases for all parties if less users participate, albeit the effects are felt disproportionately more by the smaller group. For the US, this disadvantage is borne economically in increased transaction costs of routing traffic and email, as well compliance with multiple technical standards. Most importantly, it sets back Western foreign policy interests for an Internet that can export the values of transparency, free expression and economic development.

However, from a practical standpoint, the key challenge facing ICANN isn't a country dropping out, but countries being so enamored with ICANN that the Internet gets smothered in their embrace. Like the curse of Othello, the risk isn't that of not loving enough, but too much. That governments try to become so involved that they harm the Internet's openness is a real risk.

As an observer of Internet governance for almost a decade, I take a moderate view. I don't think the issues surrounding Internet governance are so drastic that extreme positions are likely to seriously emerge for long. Instead, I believe that the world can settle these matters as it does in so many other realms – with difficulty, with discomfort, gradually and never perfectly. But eventually, well enough.

# # #

This essay, submitted as a background paper to the United Nation's Information and Communications Technology Task Force global forum in March 2004 in New York, is based on a seminar the author presented at the National Center for Digital Government at Harvard University on March 16, 2004.