Leaky Boundaries

Dan Hunter and Mary Wong
Leaky Boundaries

Dan Hunter and Mary Wong

Abstract

It was once thought that cyberspace was a separate jurisdiction, and that the nation-state’s power to govern online behavior would be usurped. This approach was quickly reversed, and the received wisdom is now that cyberspace mounts no new challenge to the state. We suggest that the received wisdom has been accepted too blithely. We argue that the next few years will see mounting pressure on the nation-state from cyberspace. We do not agree with the cyberspace exceptionalists in suggesting the emergence of a wholly separate jurisdiction for cyberspace. Instead we suggest that the entire fabric of mutually-exclusive territoriality is under threat. We explain how international relations currently views this trend away from sovereignty, and present some novel cyberspace institutions that present new challenges to state sovereignty. We conclude that states like Singapore can no longer maintain the same assumptions about sovereignty that they have held to date.

Document Control

Public Beta Revision 0.1, Wednesday, December 22, 2004. This is a non-canonical draft. It goes without saying that you may cite to it, but this document may not represent our final view.

This document is released under the Creative Commons Attribution License, http://creativecommons.org/licenses/by/1.0/ This means you may do anything you like with this document as long as you appropriately attribute it to its authors.
Leaky Boundaries

Dan Hunter and Mary Wong

The principle of all sovereignty resides essentially in the nation. No body nor individual may exercise any authority which does not proceed directly from the nation.

—Declaration of the Rights of Man

Oh, the leaky boundaries of man-made states!
How many clouds float past them with impunity;
how much desert sand shifts from one land to another;
how many mountain pebbles tumble onto foreign soil in provocative hops!

—Psalm, Wislawa Szymborska

Eight years ago it seemed that the commercial success of the Internet would lead to profound changes in our understanding of the boundaries of the nation-state. Influential scholars, most notably David Post and David Johnson, suggested that cyberspace challenged the state’s exclusive control on regulation and that for reasons both normative and descriptive, we would begin to see the emergence of autonomous zones in cyberspace where the state would not, should not, or could not intrude. This view, which came to be known as “cyberspace exceptionalism” suggested that the

---

1. Article 3, Declaration of the Rights of Man, National Assembly of France, August 26, 1789.
proliferation and ease of cross-border transaction using the internet not only would make nation-state regulation ineffective as a descriptive matter, but suspect and probably illegitimate as a normative matter. They suggested that cyberspace would increasingly come to be viewed as a separate jurisdiction that would (or should) be granted autonomy from the geographically-delimited system of laws that we have inherited as a consequence of the Treaty of Westphalia.

The views of the exceptionalists quickly came under fire. On the normative side, scholars like Neil Netanel argued that treating zones of cyberspace as independent of national systems would be likely to create democratic problems of voice and control. On the descriptive side, Jack Goldsmith argued that cyberspace posed no new problems at all. He argued that our traditional tools of jurisdiction and conflict of laws could answer any problems that cyberspace could present: after all, in the end, all these actions that occur in cyberspace still involved a person who was physically present in some real-space jurisdiction and who was subject to the Westphalian sovereign within that jurisdiction.

From a purely pragmatic perspective, it looks like the cyberspace exceptionalists lost. We haven’t witnessed the emergence of a separate jurisdiction for cyberspace, and states cheerfully regulate, censor and control cyberspace much as they have any other communication medium before it. So courts consistently rule that they have power to adjudicate cyberspace disputes that involve foreign parties. Many states control what their citizens can access on the net. And states are now using various technological features of cyberspace—including control over network engineering, and regulation of internet intermediaries like search engines and ISPs—in a

5 Johnson & Post, Law and Borders, supra note 2_


8 Id.


reasonably-successful effort to maintain regulatory control.\textsuperscript{12}

In cyberlaw circles, therefore, the received wisdom is that the sovereign primacy of
the state is unchallenged, and that the foundational assumptions of mutually-exclusive
jurisdiction and sovereignty is unchanged. We suggest that this view is simplistic and
wrong. In the paper that follow we map out some of the challenges to sovereignty that
cyberspace poses for nation-states, especially nation-states such as Singapore. Unlike
the traditionalist account that suggest that the relationship between cyberspace and
the nation-state is now resolved, we suggest that the next few years will see mounting
pressure on the nation-state from cyberspace.

Rejecting the traditionalist account does not mean that we cleave to the view of the
cyberspace exceptionalists that we will (or should) see the emergence of a wholly
separate jurisdiction for cyberspace. Indeed, the point of Part I of this paper is to
demonstrate that mutually-exclusive jurisdiction fails to recognize the intertwined
relationships that mark current understandings of international relations. The
cyberspace exceptionalist suggestion that we separate cyberspace from the real world
is an example of the fundamental problem with jurisdictional doctrines. We no longer
can separate intra-state “domestic” policy from inter-state “foreign” policy. The basis
of jurisdiction—that territorial borders between states are meaningful delimitations on
the legitimate exercise of authority—no longer holds. The answer therefore is
definitely not to introduce another separate jurisdiction that suffers from the same
leaky boundary problem as the real world. Rather the answer is to craft a response to
jurisdiction that is not willfully blind to the realities of globalization, international
trade, multi-national corporations, sovereignty-free actors, and so on.

This short paper cannot hope to craft all the elements of this response. But we can
explain how previous accounts of cyberspace jurisdiction fail. In Part I therefore we
present an account from international relations of why mutually exclusive jurisdiction
is a fiction, and why leaky boundaries are now the norm. Then in Part II we outline
some features of cyberspace regulation that demonstrate how it is contributing to the
ever-increasing porosity of those borders. We conclude with some observations about
what this means for regulators and governments in states like Singapore.

\textsuperscript{12} See e.g. Joel Reidenberg, \textit{States and Internet Enforcement}, 1 U. OTTAWA. TECH. L. J. 213 (2003-4).
I. IN THE FACE OF FRONTIERS

Need I mention every single bird that flies in the face of frontiers or alight on the roadblock at the border? A humble robin—still, its tail resides abroad while its beak stays home. If that weren’t enough, it won’t stop bobbing!

Among innumerable insects, I’ll single out only the ant between the border guard’s left and right boots blithely ignoring the questions “Where from?” and “Where to?”

—Psalm, Wislawa Szymborska

The sovereignty of the nation-state has, since the Treaty of Westphalia, represented the basic framework by which we understand international relations. The political and economic order of the world has been divided into these state-centric units of authority, to the point where it is hard to imagine an international order without such a framing principle. But the geography of territorial sovereignty, as a mode of political organization, is socially constructed rather than naturally given. It is important to understand how this social construct came to be, so that we can recognize why the sovereignty of the state has come to be threatened. And an understanding of the development of territorial sovereignty will begin to explain our reluctance to recognize quite how we can reconceive sovereignty to accord better with the modern realities of leaky boundaries.

There are both cognitive and material bases to the geographic organization of politics and economics, but let us begin with the cognitive components. How space is conceived and imagined is critical in determining its role as a mode of political organization. The revival of Ptolemaic geography in the 15th century and the development of modern maps of both Europe and the globe allowed visualization of space as delineated territory. Up until this period, maps reflected the way in which people saw the world: as a series of relations between the individual and his or her feudal, mythic or religious affiliation. It mattered little that one lived in what we would think of as “France” or “Italy”. What mattered most was one’s relationship with the lord, whether this be a feudal liege or a deity. Maps reflected this quotidian “reality” until a shift on the 15th century transformed map-making from symbolic representations of these relationships to objective depictions of “geography.”

13 Quoted in ROSENAU, supra note 2, at 451
development of fixed single point perspective in art resulted in representations of scenes and individuals as “seen” from the viewpoint of the observer. Single point perspective applied to map making and our understanding of geography involved the objectification of space and spatial relationships as “seen” from the position of external observer. The glimmerings of modernity—certainly the beginning of modernity in international relations—became apparent only when people began to see themselves from an external, objective position.

While maps can lead and constrain understanding, they more typically represent the way social realities of our understanding of the world. The medieval to modern transition involved the territorialization of politics, and the maps of the era reflect this change. The emergence of modern territorial politics marked a fundamental change from the interlaced medieval system of overlapping and interwoven authorities, diffuse “borders,” and authority based on a Christianity-defined system of inclusion. Prior to the acceptance of the Westphalian system, there existed no distinction between the internal and the external, or the domestic and the international. The emergence of the nation-state was necessary for us to even understand the concept: “internal” to what? “external” to what? It was only when the state overthrew the old order of fluid and overlapping sovereigns that we could understand the idea of mutually exclusive territorial jurisdictions, meaningful borders, and a clear hierarchy of power based on the primacy of the singular authority of the state.

Thus, the system of territorial states, of mutually exclusive territorial jurisdiction as the modern mode of political and economic organization, stems from significant cognitive changes of early modernity. But this system also reflects strong material changes that occurred during the shift from the medieval mode of non-territorial organization. During this time there arose a need for centralized power and geographically limited polities that, to this point, hadn’t existed with quite the same force. In network terms, there was a shift in the relative importance of the nodes and the relations between them. In medieval Europe, the relations dominated and there were interwoven relations among various levels and types of authority. So, for example, the authority possessed by a secular feudal lord was intertwined, but independent of, the authority of religious figures like the bishops, cardinals or pope. This was an environment where, in geographic terms, the nodes themselves were ambiguous, shifting and not overly important. But as the modern era progressed technologies of communication and transportation demanded greater geographic and

---

central control. The patterns of control and authority shifted, as the scope of communication, economic contact and markets expanded. In time these came to be the centerpieces of the nation-state, which was defined spatially according to this new conception of national geography.

So it is that there were cognitive and material foundations to the rise of the state, and the transition from the medieval to the modern. The same is true in the environment in which we now find ourselves. The transition from modern to post-modern modes of political and economic organization also has both cognitive and material bases. With the development of modern communications and transport—especially the Net, but more generally the panoply of communications devices that instantly shrink distance—it is no longer evident that we hold a single point perspective on the world. Spatial relations are less meaningful cognitively as time compression has resulted in spatial compression; or perhaps we might frame this as a fundamental acceptance that space is irrelevant. How we perceive individuals and “places” may be a function of how easy or difficult it is to contact them or how long it takes; there may no longer be a single objective depiction of space as seen from the “viewpoint” of the observer.

With the advent of the Net, we may – at least in some sense – be returning to the moral equivalent of medieval depictions of space as symbolic rather than objective. Few of us really understand what happens when we hit the “send” button or “where” the message goes or even “where” the recipient is. We may be moving towards a visualization of space in networked terms as relationships between nodes rather than nodes fixed firmly in two-dimensional geographic space.

But as with the rise of the state and modernity, the cognitive foundation of post-modern conceptions of sovereignty is perhaps less significant than the material bases. Here, the modern to post-modern transition is defined by the technologies of communications and transport that are moving towards the elimination of the distinction between internal and external transactions. So, for example, it is commonplace to log onto a website with a domain name that is not geographically delimited—<.com> say, or <.biz>—and purchase a watch, download music, or read an article. Not only may that site be physically resident almost anywhere on earth, but through the electronic terms of service, you may be contracting based on the laws of, again, almost any country on Earth.

But beyond the influence of cyberspace, the last few years have been marked by the erasure of the concepts “internal to the state” and “external to the state” as meaningful
political constructs. These new technologies, and especially the Net and the digital economy, have markedly increased the importance of the relations between nodes as opposed to the importance of the nodes themselves. The volume of transactions of all sorts has increased dramatically to the point where flows are overwhelming spaces. Borders are only meaningful political constructs if they are effective, if they serve as barriers. Space and geography are not viable modes of political-economic organization if flows dominate. Thus the modern to post-modern transition replaces the geographical organization of international politics and economics with a networked mode of organization.

This is a fundamental change. There are three basic organizing requirements for the recognition of nation-state sovereignty. It requires discrete and meaningful borders that delimit the state, and separate it from other states. It requires a conception of external sovereignty, that is, comprehensive and mutually exclusive territorial jurisdiction based upon mutual recognition. It needs internal sovereignty, which is to say autonomy and lack of competition domestically: the state must be supreme domestic authority. And there must exist a clear demarcation and separation between internal and external or foreign and domestic. But these assumptions no longer apply, and critical changes that have occurred in the basic territorial basis of jurisdiction and international relations. James Rosenau identifies this as a radical expansion of the boundary between the issues that the state used to characterize as domestic policy and that which was thought of as foreign policy.\(^{16}\) This zone he calls the “Frontier” and he demonstrates how mutually exclusive territoriality no longer exists along this new wide political space.\(^{17}\) This change has been wrought by a series of fundamental changes including: an increase in the ability of people to process and make decisions in relation to world events that affect their “domestic” interests; an increase in their ability to be involved in international affairs; a change in locus of authority from the state to a series of actors—multi-national companies, sovereignty-free civil society groups, local political organizations that span state boundaries, and so on—whose spheres of authority intersect with the state and whose authority stems not from a leviathan-like hegemony but on performance-based legitimacy; and the overall structure of international politics which has ceded power away from the state, both to local actors and supra-national actors.\(^{18}\)

---

\(^{16}\) ROSENAU, supra note 2.

\(^{17}\) Rosenau is not the only scholar to suggest the waning of the sovereign power of the state.

\(^{18}\) ROSENAU, supra note 2, at 59 et seq.
The limits on state sovereignty are present in many contexts, but are particularly noticeable in the arena of humanitarian intervention. It was once the case that states were completely autonomous, and involvement in foreign humanitarian concerns was at the convenience of the state. Now, states are obliged to go along, caught up in obligations that are imposed on them by domestic political movements, sovereignty-free civil society groups like the Red Cross/Crescent or Medecins san Frontières, and international pressure through the United Nations. Of course, this is not to say that states have no sovereignty at all, just that the political space that spans the domestic and the foreign has radically expanded.

The conclusion of this is both radical and simple: borders are no longer meaningful constructs, the distinction between domestic and foreign is losing meaning, and there are now multiple authorities in the system with overlapping spheres of authority. Inter-jurisdictional transactions and conflicts have increased to the point where a system based on mutually exclusive discrete territorial jurisdiction is no longer viable in the long term, and it is increasing difficult to locate actors, transactions, firms etc. in two dimensional geographic space. In summary then: we are in transition from a geographic to a networked mode of political-economic organization. In a networked environment, it is the relations between the nodes rather than the characteristic and location of the nodes themselves which dominates. Given the emphasis on flows rather than spaces and the marked increase in inter-jurisdictional, relative to intra-jurisdictional, flows and conflicts, geography has become problematic as the mode of political and economic organization and thus as the basis for legal jurisdiction.

With this lesson in mind we can turn to the new cyberspace actors which are contributing to the expansion of the Frontier, and which are providing new challenges to the sovereign authority of the state. In the Part that follows we examine the role of ICANN, and how it provides a new form of legislature and judiciary that contributes to the erosion of state sovereignty (especially for states such as Singapore).

---

19 ROSENAU, supra note 2, at 217 et seq
II. Chaos Prevailing

Oh, to register in detail, at a glance, the chaos prevailing on every continent!
Isn’t that a privet on the far bank
smuggling its hundred-thousandth leaf across the river?
And who but the octopus, with impudent long arms, would disrupt the sacred
bounds of territorial waters?
—Psalm, Wislawa Szymborska

As discussed above we have never really had a clear divide between domestic and
foreign policy, and the concept of state sovereignty has never been absolute. But the
twentieth century was an era when it became obvious that state sovereignty was
withering: nation-states became joined in a web of inter-relationships in trade,
commerce, and defense. This was the era when we witnessed the rise of international
law. There was the incessant march of globalization, especially in international trade
but also obvious in the transmission of political ideologies favoring democracy and
capitalism. There emerged multi-state republicanism and cooperation of various
forms, evident in institutions like the European Union, the North American Free
Trade Agreement, and the Association of South East Asian Nations. Though these
challenges have expanded the boundary of the Frontier, their effects are reasonably
well-known. States have found some means of mediating these challenges to
sovereignty, including representation in decision-making bodies, or a voice in relevant
consultative institutions. While these ameliorating mechanisms are not perfect—or
even very good—they are fairly well-documented.

However cyberspace allows a number of new types of challenges to state sovereignty
that are not well-recognized by state actors. The challenges we describe here can be
explained in terms of law-making and adjudication. They can be found in two of the
non-state systems that look to regulate aspects of the internet: the Internet
Corporation for Assigned Names and Numbers (ICANN), and the Uniform Domain
Name Dispute Resolution Policy (UDRP). In the sections that follow we explain
how these institutions widen the Frontier significantly, and why they represent new,
unrecognized challenges to state sovereignty.

A. Law Making and Policy Making Institutions

As is, by now, well-known, ICANN is a private, non-profit corporation that came into
being in 1998 and since then has sat at the highest level of the technical and regulatory processes for domain names.\textsuperscript{20} It has been extraordinarily successful in maintaining control of a messy, fast-changing, and politically-charged environment. For example, it quickly grabbed control of the registry function from the commercial operator NSI, and it presided over the decentralization of the registration function in the generic top level domains in the face of an industry monopoly player. It also weakened the power of incumbent domain name owners by introducing new generic domain name spaces, and created a dispute resolution system that panders to trademark interests but which is also the most significant change in supranational adjudication in the last century.\textsuperscript{21}

In its brief life ICANN has weathered all manner of criticisms, including charges that it is undemocratic, biased, unrepresentative, lacking in transparency, unaccountable, and so on.\textsuperscript{22} Yet its control over the domain name system is unchallenged. And most interesting for this paper, criticism of ICANN has rarely been by state actors that one would assume would be against the sovereign challenges that a trans-national, private regulatory actor mounts to individual states. Nation-states have been slow to attack what amounts to the private government of the internet.

ICANN has, from time to time, argued that it is merely a technical body and that it doesn’t exercise regulatory power. These claims have been effectively rebutted by critics like Froomkin and Mueller, and now can no longer be given much credence. But beyond the observation that ICANN is the dominant law-maker for the domain name system, it is important to recognize that it makes law without the control of nation-states. Decisions made by ICANN, including many of those mentioned above, clearly involve the exercise of what we would ordinarily consider to be sovereign power—at least within the narrow-but-significant confines of the domain name system—that ordinarily are under the purview of the state. This is remarkable, but the challenge to sovereignty doesn’t stop there. Not only is ICANN making the rules for the governance of the domain name system, it has created an adjudication mechanism for enforcing some of its rules, and has effectively created an independent supranational judicial system to administer it rules.\textsuperscript{25} Clearly there is no other body, either at the international, national or local level, which has control over the domain


\textsuperscript{21} See infra Part II.B.

\textsuperscript{22} For an account of why these views are mistaken see Dan Hunter, \textit{ICANN and the Concept of Democratic Deficit}, 36 Loy. L.A.L.Rev. 1149 (2005)

\textsuperscript{23} See infra Part II.
name system. Nation-states have clearly ceded their sovereign authority within this realm.24

This observation has not been lost on states, but they have had little opportunity to change the independence of ICANN. While it is possible for a state to remove itself from the internet or maintain state control over internal access to the net—that is, essentially forbidding its citizenry from using the network,25 filtering certain types of content or sites,26 or setting internal rules for the use of the net27—it is not possible for any one state to control the development of the internet or ICANN's management of the domain name system. It has been suggested that some states could band together to create and maintain a separate authoritative root,28 but the US first-mover advantage and the coordination costs of this move make it essentially impossible.

ICANN has therefore been largely unchallenged for six years, but its future is less certain. A number of states have introduced a long-term plan to wrest control of the domain name system away from ICANN29 by transferring it to an organ of the United Nations, the International Telegraphic Union. The ITU has recently convened a World Summit on the Information Society (WSIS) which was intended to provide representation of nation-states in various aspects of the internet. The plenary sessions at the WSIS has demonstrated that national governments seek a much tighter control over aspects of the Internet that they see as affecting their sovereign interests. This includes the ccTLD system, but also includes other aspects of internet governance such as architecture, control, finance, and the like. Representatives of France,

---

24 The discussion here is focused on the generic top level domains (gTLDs) such as .com and .net. The country code top level domains (ccTLDs) operate in a slightly different manner. Nonetheless, as we examine below, ICANN remains the sovereign power even in ccTLDs, notwithstanding the involvement of various nation-state actors in ccTLDs.

25 North Korea, for example, removed itself completely from the internet. See REPORTERS SAN FRONTIERS/TRANSFERT.NET, ENEMIES OF THE INTERNET, 79 (2001).

26 For example, Saudi Arabia, and China. See REPORTERS SAN FRONTIERS/TRANSFERT.NET, ENEMIES OF THE INTERNET, 87 (2001); Zittrain & Edelman, supra note ___.


Germany and other countries have taken the opportunity to criticize the role of ICANN and the US, and the stage was set to reëxamine sovereignty in the domain name system. From this was formed the Working Group on Internet Governance whose ambit includes may include matters as wide-ranging as spam and cybersecurity, but is clearly positioning itself to take over ICANN’s domain name responsibilities. For various reasons this is unlikely to be quite the success that the states envision. WSIS is unlikely to be able to supplant ICANN, since ICANN has already foreshadowed that it will resist these attempts and may even make itself less accountable to national interests. And if WGIG is successful, it is as likely to be as great a challenge to national sovereignty as the body it seeks to replace.

Given the challenge it presents to national sovereignty, and the heat and scale of criticisms against it, it is somewhat surprising that ICANN has managed to remain autonomous for so long, and that it is only recently that WSIS has emerged as a potential challenger to ICANN’s control over the domain name system. Perhaps, the most plausible reason why ICANN has survived can probably be traced to its peculiar position. Its control of the domain name system is based on its contract with the United States government to provide such services, and so for the purposes of many states, ICANN seems to speak for US interests. Challenges to the hegemony of the US system are not just about the international Realpolitik of a small nation-state debating the only remaining superpower. For the purposes of the domain name system the US effectively “owns” the internet because it retains effective control over the A root server. As a result, other nation-states have little power to influence


An issue present in many arenas in bilateral negotiations between the US and other states, but particularly obvious in the concession made in Free Trade Agreements between the US and Singapore, and the US and Australia.

And indeed for much of control over other regulatory elements of the internet.

Markus Müller, Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet, 15 Fordham Int. L. 1 (2005, forthcoming), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=685104, at *7-11. Mueller also notes that US “ownership” of the network is not limited to ICANN’s hierarchical control of the domain name system, but is also based inter alia on ICANN’s effective control over IP addressing, coordination
overall US policy, as it is reflected in ICANN’s decision-making. From the perspective of nation-states like Singapore, ICANN can therefore be likened to the US government. Of itself this is remarkable; a private corporation is providing the regulatory function of the US. But in international political terms, it is more surprising that states seem to have accepted US sovereignty over the network for so long.

Beyond this, there is another component of the domain name system that implicates national sovereignty more strongly: that of the domain names which involve country code top level domains (ccTLDs). These ccTLDs are the ones which are directly associated with geographically-delimited states and include .au (Australia), .sg (Singapore) and other commercially valuable domain-spaces like .tv (Tuvalu) and .to (Tonga). Because these domain names are so closely identified with the nation-states, it is unsurprising that states have taken steps to control these namespaces. In a recent study, Michael Geist reports that a large number of nation-states control their corresponding ccTLD namespace through various means, most notably direct administrative operation of the registry, or effective state control of the registry operator.

ICANN displays an acute awareness of the relationship between perceptions of nation-state sovereignty and ccTLD namespaces. This is to be contrasted with ICANN’s attitude in the gTLDs, and more obviously, the attitude of the precursor to ICANN, which was less sensitive to the issue due no doubt to the absence of government involvement in most early internet decisions. The father and long-time

difficulties for other states to secede from US control, and on control conferred by intellectual property interests. See Müller, at *14-33.

See generally Yu, The Neverending CCTLD Story.

One commentator goes so far as to suggest that each country’s ccTLD is a fundamental component of its national sovereignty and “a vital national interest.” See Kenneth Neil Cukier, “Eminent Domain: Initial Policy Perspectives on Nationalizing: Country-Code Internet Addresses,” http://inet2002.org/CD-ROM/lu65rw2n/papers/g03-b.pdf, June 2002, 1.

Michael Geist, Governments and Country-Code Top Level Domains: A Global Survey, Preliminary Report, 4, (December 2003), available at www.michaelgeist.ca/geistgovernmentctlds.pdf. The report has come under criticism from the Council of European National Top-Level Domain Registries, for its methods and purported ideology. See Tim Mertens, CENTR Reply to ITU Study on ccTLD Governance, CircleID, Jan 9, 2004, available at http://www.circleid.com/article/421_0_1_0_C/. And of course Professor Geist has responded. See Michael Geist, The Debate Continues: Geist Reply to CENTR Response, CircleID, Jan 9, 2004, available at http://www.circleid.com/article/424_0_1_0_C/. The argument can be seen as indicative of the animosity between those like CENTR who support a privately-constituted network administrator (ICANN) and those who seek greater involvement by nations-states through typical international legal institutions (ITU). The substance of the debate is irrelevant to the issues under discussion here, since we suggest that as far as ccTLDs are concerned, the distinction is meaningless.
guardian of the DNS, Jon Postel, initially delegated control of ccTLD registries to a “responsible person”, usually the first person who asked for the job who happened to be associated with the relevant country.41 Later, IANA42 undertook control of these namespaces, and its delegation and administration policy made clear the nature of internet governance circa 1994;43 the ccTLD namespaces were to be managed for the internet as a whole, not just for the relevant country although its interests counted,44 and the normative criterion for appropriateness of delegation was consensus.45 Of course, IANA wasn’t actively looking to pick a fight with nation-states, and so in its delegation of control of ccTLDs it noted that it took “…the desires of the government of the country very seriously, and [would]…take them as a major consideration in any transition discussion.”46

ICANN, on the other hand, has not upheld this normative conception nor has it privileged the internet community generally over the nation-state: it has consistently deferred to the relevant state in determining who should have registry control over the ccTLD namespace. One of the most influential of its advisory committees is the Government Advisory Committee, which has representatives from nation-state governments.47 Thus, for example, where there was a dispute over control of the <.au> namespace between the government of Australian and the person who was granted the initial registry control, ICANN had little hesitation in summarily transferring control to the Australian government. This was controversial to those who had a cyberlibertarian viewpoint, and those who are concerned about the accountability of ICANN as a regulatory body. As much as possible ICANN seeks to remove itself from conflicts between the affected nation-state and other parties claiming control of the ccTLD, and there are a number of cases where this has stopped any re-delegation.

41 See Mueller, RULING THE ROOT, 88-9; Yu, Neverending CCTLD Story, 2.
42 The Internet Assigned Numbers Authority. This was effectively Jon Postel. See Mueller, RULING THE ROOT.
43 The representative statement of this period comes from the US Government itself, whose White Paper stated that "neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses.”
45 On the problems of resolving political issues by internet consensus see Hunter, supra note ____.
46 IANA, ccTLD News Memo #1, (October 1997), available at http://www.iana.org/cctld/cc-tld-news.htm
47 Example of importance, the GAC Principles, page 5 of Yu.
It is unsurprising in international relations for an international political institution to demonstrate its allegiance to the established international political order. Indeed it is revealing of ICANN’s role that, to date, ccTLD namespaces have generated little difficulty, and the only time that ccTLDs forment significant arguments is when the sovereign political authority for a given state is in question.\textsuperscript{48} So the ccTLDs for Afghanistan, Iraq, and Palestine\textsuperscript{49} become freighted with the kind of international politicking that is familiar from UN debates, and ICANN typically defers decision-making until these issues are resolved at the international legal level.\textsuperscript{50}

It is clear that, as far as ccTLDs are concerned, ICANN operates by the same sorts of structural and procedural norms that apply to international institutions formally-constituted under the UN. But it is wrong to suggest that demonstrates that the states actually retain sovereignty, even in this arena. States have control over their ccTLD at the pleasure of ICANN, not as independent sovereigns. For example, the Geist reports notes that number of states have enacted legislation, or have threatened to enact legislation, in an effort to control their ccTLDs.\textsuperscript{51} While this is clear evidence that the state seeks to have control over its ccTLD,\textsuperscript{52} it does not mean that those attempts at sovereign control are effective. Within the clear confines of its own boundaries, a state can legislate to grab control of the ccTLD registry; for example, if a legacy registry operator refuses to hand over the keys to the ccTLD registry. But it is still dependent on the good graces of ICANN to recognize this redelegation, and the state has no power to compel ICANN to do so. It seems then that the particular genius of the management of the ccTLD system is that it provides nation-states a degree of ostensible control, without affecting the actual control of the domain name system. For even though the zone file for each ccTLD is under the control of the relevant state (either directly or through a trusted intermediary), the A root controls the overall availability of the ccTLD zone file.\textsuperscript{53} So again, the US effectively controls the entire domain name system, even that part of the system which is notionally under

\textsuperscript{48} From the earliest stages, ICANN and its predecessors disclaimed any interest in deciding the issue of statehood.


\textsuperscript{50} Geist, supra note at 4.

\textsuperscript{51} Geist uses it for this reason. Id.

\textsuperscript{52} Mueller, Ruling the Root; Markus Müller, supra note at 5-9, 14.
national control.

The conclusion here is obvious. ICANN represents a significant new challenge to the sovereignty of states, because it is both a policy-making and law-making body that is wholly private and outside the limits of effective control of any state apart from the US. It represents a new type of institution that expands the realm of the Frontier, and demonstrates the inability of nation-states to regain power over technical systems that are vital to their national interests. And perhaps most interesting, even in the ccTLD arena where ICANN has ceded notional sovereignty to the states, the reality is that this sovereignty is contingent and thin.

B. Judicial Institutions

The Uniform Domain Name Dispute Resolution Policy is a creation of ICANN, in conjunction with the World Intellectual Property Organization, but its challenge to sovereignty is slightly different to the one posed by ICANN itself. The UDRP is the policy that was crafted to deal with the problem of cybersquatting, where entrepreneurs registered domain names that included elements of well-known trademarks. Since its creation in 1999 it has disposed of thousands of cases involving domain names, mostly in the .com, .net, and .org namespaces, but also in some ccTLD namespaces where it has been directly adopted.

The UDRP is extremely unusual in the annals of adjudication, because it is untethered from national adjudication systems. Courts and the adjudication of disputes is one of the characteristic functions of sovereigns. Although private systems have, for some time, been licensed by the state, they almost always operate within the bounds of national, provincial or state jurisdictional boundaries. And there have been a small number of private, supra-national dispute resolution mechanisms, such as the London International Court of Arbitration, which are used for arbitrations involving large commercial parties arguing over issues to do with international trade. But there has never really been an adjudication process at this scale which is untethered from national jurisdictions and which adjudicates disputes involving individuals.

One of the more notable aspects affecting sovereignty here is the way in which a dispute between the nationals of one state are commonly judged by nationals of other countries. Although dispute resolution providers may try to match judges with the

---

nationalities of the parties, in many cases this is simply impossible, or not in the interests of the dispute resolution provider. Indeed, for dispute resolution providers such as the National Arbitration Foundation it will be impossible for them to appoint local judges, since they are overwhelmingly composed of American adjudicators. This means that the overwhelming majority of decisions rendered by these providers will be decided by US judges, sitting in judgment on parties from Singapore, Brazil, Estonia, or somewhere-not-being-America. These judges might be expected to apply local law to these disputes, since it is open for them to do so. However, it will come as little surprise that these judges often—indeed usually—render decisions based upon the law that they happen to know: which is to say the US law. This represents an unusual expansion of US sovereignty into the adjudication of legal disputes, which must be considered unparalleled. As against, say, multi-million dollar disputes involving international trade, cases decided under the UDRP are done quickly, with no opportunity to examine the parties, and no established body of international customs or norms to guide the decision-makers. As a result US law—and to a lesser extent other common law principles—are being exported directly into national systems that have no connection to these legal systems.

Beyond this the expansion of other legal systems into the adjudicatory space of various sovereigns, we can see the development of identifiable sovereign bodies for this type of supranational adjudication. The dispute resolution providers—especially the largest players, WIPO and NAF—are not perfectly neutral in their relationship to sovereign nations. This is, to some degree, an extension of the standard critique made of the dispute resolution providers, that they are biased towards particular interests: commentators like Michael Geist and Milton Mueller have accused the dispute resolution providers of being biased in favor of the trademark owners who bring these actions against cybersquatters. Here, the nature of the bias is different, though the process by which it takes place is the same as that proposed by Michael Geist. Geist notes that the process of allocation of judges to disputes is one of the most important

---

55 One of the providers, WIPO's Arbitration and Mediation Center, endeavors to do so, and has a large number of prospective judges drawn from many countries. See WIPO Domain Name Panelists, available at [http://arbiter.wipo.int/domains/panelists.html](http://arbiter.wipo.int/domains/panelists.html)


features of the UDRP, and yet no dispute resolution provider publishes the criteria by which is allocates judges to decisions.\textsuperscript{58} It is clear that the allocation process allows dispute resolution providers to affect the outcome of the cases, in a number of ways. First, it allows them to assign judges to particular cases who are likely (based on previous decisions) to decide the case in a certain way. Though this process may be subtle, at times it is extraordinarily blunt. For example, one of the authors (Dan Hunter) has been a UDRP judge for WIPO for the last four years, and at one point was asked to sit on a case involving a South Korean respondent, where there was a South Korean registrar of the domain name. Under the UDRP Rules, the case material can be provided in the language of the registrar, and so the documents were all written in Korean. The Arbitration and Mediation Center approached Hunter asking him to sit as a member of a three-person panelist on this case, and said that they would provide translations of the documents. When asked why the AMC didn’t appoint another panelist who could read Korean, the AMC responded that they believed Korean panelists favored Korean respondents, and so abusive registrations were made with Korean registrars in order to guarantee Korean panelists in the event that a UDRP case was filed against the registrant. While they AMC did not tell the panelists to decide a particular way, it is clear that they chose the panel based on certain expectations about the appropriate outcome. It is not ridiculous to suggest here that the sovereign interests of South Korea are implicated in a case such as this, and though it is the only one that we can speak to with direct knowledge, it is unlikely to be the only case of its type. Beyond this, the dispute resolution provider also maintains strong coercive control over it judges, and does not appear to flinch from exercising this control. Many panelists have experienced pressure from the dispute resolution providers to decide cases in particular ways, and the providers are always careful not to document these “discussions,” which always occur over the phone.

By its allocation processes and its control over the outcome of decisions, the dispute resolution providers represent a distinct supranational institution that is unaccountable to any sovereign nation. To the extent that they are accountable to anyone, it is to ICANN, since ICANN appoints them. ICANN has clearly signaled that it does not intend to remove these dispute resolution providers, as it has done nothing to control the providers even in light of significant criticism from various commentators. Since ICANN is under the control of the US government it would be surprising if it did anything to alter the UDRP, even if the sovereign interests of nation-states other than the US were affected.

\textsuperscript{58} Geist, supra note ___.

-19-
Finally, adjudication within the domain name system has the same local analog as the law making process has above. That is, each registrar for the ccTLD system is entitled to set its own dispute resolution policy, and need not adopt the UDRP. One would expect that these dispute resolution policies would reflect the specific legal environment of the local nation-state. But this isn’t so, and the vast majority of these policies are minor variants of the UDRP. For example Singapore has the Singapore Domain Name Dispute Policy (SDRP) and the SDRP is taken almost word for word from the UDRP. Since there is now a well-established corpus of UDRP decisions, it is not surprising that panelists deciding under the SDRP—who are usually Singaporean nationals—tend to follow the law that has been established under the UDRP. In this way the Frontier-established, trans-national law of the UDRP is propagated downward into the decision-making that we would ordinarily think of as forming part of the domestic legal system of the nation-state.

III. Conclusions

And how can we talk of order overall
when the very placement of the stars
leaves us doubting just what shines for whom?

Not to speak of the fog’s reprehensible drifting!
And dust blowing all over the steppes
as if they hadn’t been partitioned!
And the voices coasting on obliging airwaves.
And conspiratorially squeaking, those indecipherable mutters!

Only what is human can truly be foreign
The rest is mixed vegetation, subversive moles, and wind.
–Psalm, Wislawa Szymborska.

The Westphalian system is a remarkably durable order, that has survived the various technological and political revolutions of the last five hundred years. It is likely to survive the emergence of cyberspace as well. However, for all that it has survived these upheavals, the system inevitably changes, and assumes some of the characteristics of the new international order.

But while the system may remain, the effectiveness of any given state may change. So it is that states like Singapore need to understand how the sovereignty challenges affect their long-term ability to govern their citizens. We have demonstrated that the
distinction between the domestic and the foreign is becoming increasingly meaningless, and that new internet institutions are blurring the distinctions even further. Perhaps most interesting of all, we have suggested that the types of challenges presented by cyberspace are *sui generis*, and the typical mechanisms used by states to maintain sovereignty will not prove very effective to defeat them.

As new issues arise in cyberspace we can expect to see other institutions arise which will follow the lead of ICANN and the UDRP. It is likely then that the wide political space that is the cyberspace Frontier will become even wider.