Global Village, Global Marketplace, Global War on Terror:
Metaphorical Reinscription and Global Internet Governance

by

Nisha Shah

A thesis submitted in conformity with the requirements

For the degree of Doctor of Philosophy

Graduate Department of the Department of Political Science

University of Toronto

Global Village, Global Marketplace, Global War on Terror:
Metaphorical Reinscription and Global Internet Governance

Doctor of Philosophy, 2009

Nisha Shah

Department of Political Science, University of Toronto

ABSTRACT

My thesis examines how metaphors of globalization shape the global governance of the Internet. I consider how, in a short span of time, discussions of the Internet's globalizing potential have gone from the optimism of the *global village* to the penchant of the global *marketplace* to the anxiety of the *global war on terror*. Building upon Rorty's theory of metaphors and Foucault's notion of productive power, I investigate how the shifts in these prevailing metaphors have produced and legitimated different frameworks of global governance. In considering how these patterns of governance have been shaped in the context of a familiar example of globalization, I demonstrate that globalization has an important discursive dimension that works as a constitutive force – not only in Internet governance, but in global governance more generally.

By illuminating globalization's discursive dimensions, this thesis makes an original theoretical contribution to the study of globalization and global governance. It demonstrates that globalization is more than a set of empirical flows: equally important, globalization exists as a set of discourses that reconstitute political legitimacy in more 'global' terms. This recasts the conventional understanding of global governance: rather than a *response* to the

challenges posed by the empirical transcendence of territorial borders or the visible proliferation of non-state actors, the aims, institutions and policies of global governance are shaped and enabled by discourses of globalization, and evolve as these discourses change. In short, this thesis provides further insight into globalization's transformations of state-based political order. It links these transformations to the discursive processes by which systems of global governance are produced and legitimated as sites of power and authority.

Acknowledgements

It takes a village, says my brother, referring to the network of support that makes individual achievements possible. In the spirit of this thesis my village has had a truly global scope, with colleagues, friends, and family around the world providing the encouragement that motivated me to start this project and successfully see it to completion.

Its genesis can be located in the discussions of an eclectic group of undergraduate students at McMaster University. Their curiosity in all things 'global' led them to investigate the importance and impact of stock markets, world music, and diasporic literature. I thank my fellow 'globies,' without whom the question of globalization would never have been intriguing – and, more so, entertaining.

While the conclusions in this project are my own, they have been the product of animated debates, incisive criticism and creative observations. Mentors, colleagues, fellow graduate students and teachers have all contributed to my mediations on the nexus between globalization, metaphors and the Internet. In particular, I want to credit the past and recent conversations I've had with Jens Bartelson, James Brassett, Angharad Closs Stephens, Richard Falk, Erin Hannah, Anu Koshal, Rinku Lamba, Linda B. Miller, Tony Porter, James Rowe, Jan Aart Scholte, Matthew Sparke, Manfred Steger, Richard Stubbs, Allona Sund, and Peter Wilson. Markus Kornprobst, Vincent Pouliot, Ruben Zaiotti and the collaborators in the Metaphors of Globalization Workshop have allowed me to engage the question of metaphors with breadth and analytical sophistication that would not have been possible on my own. Robert Guerra, Jeanette Hoffman, Milton Mueller, William Drake, and, in a different way, Gillian Youngs have provided guidance on questions about information technology, communications and International Relations – without which my study of the

Internet would not have at all been possible! In the final stages of this project, Philippe Bonditti and James Der Derian provided the good humour and sound advice necessary to keep the task at hand in perspective.

Support, of course, always has a material dimension. I have benefited from the support of several Ontario Graduate Scholarships and a Social Sciences and Humanities Research Council of Canada Doctoral Scholarship. I would like to thank the University of Toronto's School of Graduate Studies and the Department of Political Science for travel funding that supported my fieldwork. John Fraser, Anna Luengo and Geraldine Sharpe at Massey College provided support both for conference travel, but also resources that facilitated a productive work environment. In the later stages of my research, I was beneficiary of an Andrew Mellon-Sawyer Doctoral Fellowship as part of the 'Globalizing the Americas' Seminar. I thank Rick Halpern and Kenneth Mills for inviting me to participate in this seminar, and allowing me to discover the broader context in which my work could be situated and the diverse set of issues to which it can be applied. I would also like to thank Joan Kallis, Graduate Administrator in the Department of Political Science. Her efforts in keeping both the academic and logistical dimensions of my work on track have been endless. Tina Lagopoulos at the Centre for International Studies in the Munk Centre also deserves credit for administrative support – and friendship – that have allowed my research to progress without major hiccups.

The sacrifices that have allowed me to complete this dissertation have not only been my own. My friends have dealt with my absence and invisibility with great compassion and understanding, sending 'good vibes' via email if necessary when I was in the depths of writing. Dan Giang, Nili Issacs, Juliet Mbiti and Anita Mehta, in particular, have reminded

me that friends are not to be taken for granted. My family has contributed in ways that cannot be fully expressed here. As the line between friend and family increasingly blurred, Meera and Ram literally took me into their home and provided the space (and television) necessary that facilitated the most productive stages of my work. Anjana and Sirish Shah have appreciated and taken a keen interest my research, even when it was not always clear what it was that I was doing.

My village, of course, has its roots in my immediate family. Jagesh and Sangeeta can hopefully see the value of their advice and tolerance during my numerous moments of 'crisis'. By asking me what it 'means' to do a thesis and to do research, Anjali has forced me to be accountable about why what I do matters – not only to me but to a five year old. Karina provided the impetus to complete this project in a timely fashion; from the perspective of a two- year old, I was "too old" to still be in school. My parents, Urmila and Vijay Shah, have borne the brunt of the sacrifices that have made any of my academic accomplishments possible. Filling bank accounts and refrigerators and consoling my many moments of anxiety have been the least of their efforts. My academic curiosity and inquisitiveness is a result of their example and a credit to their support of asking and exploring any kind of question, no matter how esoteric it may at first appear.

This thesis would not have been possible without the guidance and support of my supervisory committee and members of the Department of Political Science at the University of Toronto. Ronald J. Deibert has seen this project evolve from a set of broad interests to clearly defined and empirically grounded research questions. Emanuel Adler has read through wandering drafts and provided the compass that has allowed me to find engaging and intellectually satisfying propositions and methodologies. Together, they have provided an

uncompromising supervisory team. The least of their efforts has added precision to my work; more importantly, they have encouraged me to be both a critical and a creative scholar. Nancy Kokaz continually fails to appreciate the value and contribution of her incisive questions and demands for analytical clarity. Her 'invitations to be more assertive' about the uniqueness of my contributions have allowed me to find my own voice and find the value – both academic and practical – of my theoretical and empirical explorations. Steven Bernstein has provided advice from the sidelines. However, his unique insights and innovative provocations on questions of global governance and legitimacy have directly informed my own theory of 'globalization as global governance'. Although not formally on my committee, I would like to thank David Welch and Louis W. Pauly. David has taught me the value of healthy academic debate and demonstrated a true intellectual capacity to respect and engage diverse perspectives. David has also been a confidence builder – reminding me that I had indeed chosen the 'right path' during those moments of anxiety that accompany thesis writing and research. Lou has shown respect to and appreciation of a younger and less experienced scholar that I surely do not deserve. If I am to have a successful academic career, it will in part be because of his faith, encouragement and practical advice (and, office space!). Finally, I'd like to thank Lene Hansen at the University of Copenhagen. The advice of Lene's thorough and constructive review of my thesis is not reflected in the pages that follow. However, her comments and suggestions will allow me to build on this work and develop it with greater analytical depth and methodological rigor.

Three people in particular deserve special mention. They have accompanied me on this journey, sharing in its moments of joy and relief and also suffering the anxiety of setbacks and unforeseen challenges. First, Kate Mulligan: my sounding board and closest

friend (and also a fellow globie). Kate has been my unofficial thesis supervisor. Without her encouragement, this thesis would have been long abandoned. Without her belief, it would have been much harder to keep going. Second, Jai Shah: few graduate students are blessed with partners who can appreciate the value of their work, volunteer research assistance, endlessly provide emotional support, and read through their work with an eye to analytical precision that improves it intellectually. He has shown incredible patience during most demanding moments of this process and has been the first to appreciate and celebrate in its successes. The quality of the final project is a testament to his love and intellectual engagement.

Finally, I would like to thank William D. Coleman, who introduced me to the world of globalization theory almost a decade ago. The value of this work should be credited to his mentoring and friendship, and it is to his inspiration that it is dedicated.

NS

Toronto, 2008

Table of Contents

Introduction

Globalization and Discourse

> What … is the relationship between the concrete processes and institutions of globalization – 'global' brands and firms, institutions of 'global' governance, globalizing technologies, etc. – and the various stories, myths, ideologies and rhetoric that surround them? To what extent do the latter affect the former rather than merely describe them?
> ~ Angus Cameron & Ronen Palan, *The Imagined Economies of Globalization*

The Internet has become emblematic of globalization. Its planetary system of fibre optic cables and near-instantaneous transfer of information are considered, by many accounts, key to understanding the transformation of world order and the ability to imagine the world as a single, global space. As Goldsmith and Wu (2006, p. 179) note, "the Internet has widely been viewed as the essential catalyst of contemporary globalization, and it has been central to debates about what globalization means and where it will lead."

One assumption in these analyses is that the planetary reach of the Internet's decentralized network of networks compromises the traditional source of political power, the sovereign state. New actors – from activist movements to financial authorities to terrorist operations – have been empowered, and new networks of authority have been created that operate beyond the borders of the state in a novel global context. Amongst the diverse forces associated with globalization, then, the Internet symbolizes how the constituent units, actors and institutions of world politics have shifted from the international system of *sovereign* states to a post-sovereign *global* political field (Cairncross, 1997; Castells, 2000b; Dodge &

Kitchin, 1998; Friedman, 2000, 2005; Stephen J. Kobrin, 2002; Nye, 2004; Ohmae, 1990, 1995; Rosenau & Singh, 2002).

This view of the Internet as a manifestation of globalization typically focuses on sovereignty's 'territorial' dimensions. Because the Internet is not easily bound by the physical geography and legal boundaries of states, political order is transformed from conventional territorialist geometries of political authority to more global ones. Yet an alternative view holds that while the territorially bordered nature of political authority is one of sovereignty's signature features, sovereignty also has *discursive* dimensions. This view sees sovereignty as a discursively constituted principle that legitimates a particular organization of political authority, identity and community as mutually exclusive units represented by territorial states. The state, then, becomes an authoritative locus of political order not because of its territorial integrity but because of its *political legitimacy*, a normative understanding about the location (and by extension, the limits) of the field of political and social relations (Bartelson, 1995; Biersteker & Weber, 1996b; Walker, 1993; Weber, 1995).

This is, of course, not to deny that globalization in different forms has challenged the topography of conventional political life in tangible and empirical ways. Nor does it dispute that global governance partly reflects the ways in which certain dynamics and issues cannot be contained within the scope of a single, territorially defined government. However, in light of sovereignty's discursive dimensions, if globalization represents a moment of political change (evidenced by systems of global governance) then it must do more than simply transcend states' physical-territorial borders: globalization must also *de*legitimate sovereignty by offering discourses that provide different principles of political legitimacy, ones that sanction globalized forms of political authority

Without this power – without the ability to delegitimate sovereignty and relegitimate political order in some different, some *global* way – globalization lacks the capacity to transform political order. It is therefore necessary to consider how a global political field is discursively articulated, according to which normative principles, and how, if at all, they contest and change the norms of legitimacy and institutional frameworks of the sovereign states-system. In short, delineating globalization's capacity to generate a new sphere of political authority and action requires an exploration of its discursive dimensions.

Conceptualizing globalization discursively appears to be particularly pertinent when assessing the Internet's relationship to globalization. Consider the following opinions:

- *"The globe is a village and the village is global … The trend towards 'deterritorialization' produced by ICTs [information and communication technologies]… undermines the legitimacy of a political system which is territorially bounded …"*[1]

- *"As an electronically networked world economy renders borders less meaningful, jurisdiction loses significance. As markets are increasingly constructed in cyberspace, control through control over territory becomes problematic."*[2]

- *"Over the past two or three years, face-to-face radicalization is being replaced by online radicalization. [Internet] forums … have become the virtual "invisible hand" organizing terrorist activities worldwide."*[3]

Three different metaphors of globalization can be detected here: *global village, global marketplace,* and *global war on terror*. Their representations of globalization reveal that the

[1] Frissen,P. (1997). The virtual state: postmodernisation, informationisation and public administration. In B.D. Loader (Ed)., The Governance of Cyberspace: Politics, technology and global restructuring (pp. 111-125). London: Routledge.
[2] Kobrin, S. J. (2002). Economic governance in an electronically networked global economy. In R. B. Hall & T. J. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 43-75). Cambridge: Cambridge University Press.
[3] Marc Sageman qtd. in *Violent Islamist Extremism, the Internet and the Threat of Homegrown Terrorism* (United States Senate Committee on Homeland Security and Governmental Affairs, 2008).

'global' space of the Internet has been constructed and experienced in multiple ways, each suggesting different challenges and priorities for 'global' orders of governance: a harmonious world polity, a competitive global economy and a front in the fight against terrorism. They hint that the concepts of global governance and the forms it takes, emerge not only from cross-territorial flow of instant messages, email and VOIP, amongst others, but in how these flows are articulated and deployed within a certain discursive context. Thus, pointing to the Internet's ability to easily cross territorial boundaries is necessary, but appears to be insufficient for illustrating globalization's purported transformations of political order from a system of territorial states to global governance. Attention must also be directed to how the Internet's globalizing potential is situated in and shaped by discourses of globalization and their particular normative constructions of 'global' as a political space

The articulation of the Internet through different globalization discourses suggests, as Steger (2003, p. ix) claims, that "globalization is not merely an objective process, but also a plethora of stories that define, describe and analyse that very process. The social forces behind these competing accounts of globalization seek to endow this relatively new buzzword with norms, values, and meanings that … legitimate and advance specific power interests …" (see also Steger, 2004; Steger, 2005). Reconceptualizing globalization in this way forces us to consider how our knowledge and practice of globalization is informed not only by various cross-territorial empirical trends but also by "theories and images that prescribe both [their] form and consequences and our response to them" (Cameron & Palan, 2004, p. 3).

Along these lines, the question is not just how the Internet may contribute to (or be prototypical of) the genesis of systems of global governance: if the Internet is indeed

emblematic of globalization and its transformations of political order, it is equally important to ask how the Internet itself is globally governed. That is, how the Internet's globalizing capacities are influenced and enabled by discourses of globalization, how the discursive definitions of 'global' as a political space should be seen as undermining the legitimacy of sovereignty, and finally, how this implicates the way the Internet's 'globally' oriented governance institutions and practices are structured.

To address these questions, this study probes into the contexts and forces that have resulted in the articulation of the *global village*, *global marketplace* and *global war on terror* metaphors of globalization. It investigates the particular ways in which these metaphors have contributed to institutions, policies and practices of global Internet governance. Even with claims that the Internet is by definition globalizing, it is common knowledge (and ironic) that the Internet began as an instrument of state power, a product of the US government's Cold War national security objectives (Abbate, 1999; Dodge & Kitchin, 1998). Illuminating the influences that these metaphors have had on the Internet's evolution as a subject of global (rather than solely sovereign-territorial) frameworks of governance – acknowledging that the Internet's global governance principles can evolve, and exploring the ways in which they do so through the lens of changing dominant metaphors – provides a way to identify and reflect upon the discursive production of global political spaces and how this challenges and potentially changes a sovereign, territorial world order.

Of course, investigating globalization discourses could extend well beyond their possible relation to Internet governance: *global village*, *global marketplace* and *global war on terror* are more general descriptions of globalization. Still, the view that global governance can be considered the outcome of physically transcending state territorial borders

is pervasive. This understanding of globalization as a set of empirical trends that (a) compromise sovereignty by crossing over territorial borders, and (b) give rise to global governance institutions and practices, is particularly characteristic of mainstream approaches to globalization within International Relations scholarship, where the relationship between globalization and new forms of global governance has flourished as a field of study. Such a focus on the physical transcendence of borders as a measure of global governance is puzzling considering the rhetorical force and popularity of these metaphors in both scholarly and non-academic accounts of globalization. More significantly, it is problematic given that sovereignty needs to be understood not only in terms of the inviolability of territorial borders, but also as a discourse that legitimates the territorially-bounded state as a site of political authority.

The position defended in this study is that globalization is more than a set of empirical flows; globalization must also exist as a set of discourses that reconstitute political legitimacy in more 'global' terms. Exploring the role of metaphors as one element within the discursive legitimation and construction of political order, and shedding particular light on how they have influenced the Internet's global governance, I seek to demonstrate that globalization's transformations of state-based political order should be situated not only in the movement of goods, services, and information across territorial borders – but, equally important, in the way these transformations are linked to the discursive processes by which systems of global governance are produced and legitimated as sites of power and authority.

My objective is therefore to develop a theoretical and analytical framework that broadens the study of globalization to include analyses of the deployment of discourses contributing to the genesis of global political order. This genesis can be evidenced in and by

novel governance institutions and practices. The intent of this approach is neither to reduce globalization (or the Internet) to a collection of discursive elements, nor to claim that they are the only factors of consequence in explaining nascent global political orders. I certainly do not contend that discourses should be given priority over other facets of political change; political transformations are complex and must always be investigated as the unanticipated outcomes of the convergence of diverse material and social forces (Cox, 1981; Deibert, 1997b). Instead, my aim is to develop theoretical tools that identify discourses amongst the collective forces and events we call 'globalization' and reflect on the particular role they have within this matrix to affect political change. Creating space for the investigation of the relatively under-theorized relationship between discourses and globalization in International Relations scholarship can, I believe, help to better illuminate the emerging global dimensions of world politics.

In this chapter, I outline a theory of globalization as a discursive practice that operates, amongst other things, through metaphors. I begin with an overview of the extant literature on globalization and global governance in International Relations. As will be revealed, although attention to discourses is not novel, with few exceptions discourse has largely been overlooked in the discipline's study of globalization and global governance – leaving significant gaps in our account and assessment of globalization's transformative impact on world politics. The three metaphors described at the start of this chapter are some of the most immediately recognizable iconography of globalization and the Internet. It goes without saying that they have become familiar and assumed vocabularies when describing and defining globalization, and have thus come to frame our understandings of globalization and the Internet in distinct ways. Metaphors therefore extend beyond mere buzzwords, even

if at times they are circulated in overzealous popular punditry (Anderson, 2005; Friedman, 2000, 2005), and as a result provide an entry point for investigating globalization's discursive dimensions. Elaborating upon Richard Rorty's (1989) notion of *metaphorical redescription*, I propose exploring these metaphors' particular effects within the maelstrom of globalizing transformations.

Examining the role of metaphors is a pragmatic hypothesis: I hope that the lens they bring to bear on the discursive processes involved in globalization will disturb rarefied assumptions and open up new lines of investigation that can augment and improve upon existing interpretations. This applies not only to the Internet's globalizing role, but also to how we should understand and study contemporary globalization and global governance more generally.

Theorizing globalization discursively

> The surest sign that a society has entered into the secure possession of a new concept is that a new vocabulary will be developed, in terms of which the concept can then be publicly articulated and discussed.
> ~ Quentin Skinner, *The Foundations of Modern Political Thought: The Age of Reformation* (Vol. 2)

Even though the zeal with which "globalization" has occupied International Relations scholars has subsided since its height in the 1990s, references to globalization remain pervasive, even if hotly contested.[4] In studies ranging from political economy to the more conservative area of security studies, globalization is often considered a defining feature of

[4] See Weiss (1998) and Hirst and Thompson (1999). Criticisms of globalization have become more pronounced in the aftermath of the 11 September 2001 terrorists attacks, whereby the heightened security context of anti-terrorism efforts is interpreted as reinforcing the power sovereign states to protect their territorial borders (Acharya, 2007; Andreas, 2003; Gray, 2002; Sparke, 2006). In a different vein, Rosenburg (2000; , 2005) argues that globalization is nothing new, or that its moment has passed.

contemporary world politics. As former UN Secretary General Kofi Annan put it, " globalization is a fact of life" (qtd. in Foreign Policy, 2007). That it is commonplace to consider globalization as part of the everyday business of world politics makes the need to investigate globalization's discursive dimensions more urgent. How and why has "globalization" become entrenched as part of the collective vocabularies of world politics? What kind of understandings of a putative 'global' political sphere, its primary actors and institutional frameworks do these vocabularies promote (and thereby preclude)? How have these vocabularies "mapped the terrain" of the 'global' and do they legitimate certain kinds of political power (Sparke, forthcoming; Steger, 2004)?

Answering these questions is the core focus of this study. However, asking them presumes an understanding of globalization that stands at odds with the mainstream conceptualization in International Relations scholarship. Defined as the unprecedented flow of goods, services, people and ideas across the state's territorial borders, globalization is generally viewed as a set of objective trends that can be empirically tested and measured – for instance, the 'fact' of globalization is determined by examining rates of travel between countries, the number of Internet hosts and servers, and the movement of goods and services across borders and foreign direct investment as signs of deepening market integration (Cairncross, 1997; Y. H. Ferguson & Mansbach, 2004; Friedman, 2000, 2005; Held, McGrew, Goldblatt, & Perraton, 1999; Ohmae, 1990, 1995; Rosenau, 2003; Rosenau & Czempiel, 1992; Strange, 1996; Wolf, 2001). In its 2007 Globalization Index, *Foreign Policy* presented the following as "undeniable" evidence of a globalized world:

> An estimated 2 billion people witness Live Earth, a series of concerts held in 11 locations around the world to raise environmental awareness. Chinese manufacturers decorate toys with paint containing lead, and children around the world have to give

> up their Batmans and Barbie dolls. Mortgage lenders in the United States face a liquidity crunch, and global stock markets go berserk.

In this approach to studying globalization after a certain point rates of cross-boundary communication, transportation and trade "lead towards the creation of a world characterized by the dominance of political and economic systems constituted on a global scale" (Cameron & Palan, 2004, p. 30).

In light of these new kinds of global political and economic systems, globalization is traditionally studied for how it undermines – or 'unbundles' – the system of sovereign territorial states and replaces it with a new, albeit nascent, political order, evident in *globally* defined governance institutions, actors, laws and norms (Anheiner, Galsius, & Kaldor, 2001; Bernstein, 2004; Cutler, Haufler, & Porter, 1999; Y. H. Ferguson & Mansbach, 2004; Held, 1995, 2004; O'Brien, Goetz, Scholte, & Williams, 2000; Prakash & Hart, 1999; Rosenau & Czempiel, 1992; Ruggie, 1993; Slaughter, 2004). This outcome is not considered a forgone conclusion – many accept globalization as fact but do not necessarily contend that it has any transformative power; by some accounts, it even bolsters the power and authority of the state (Hirst & Thompson, 1999; Kissinger, 2008; Thompson & Krasner, 1989; Weiss, 1998). But, unsurprisingly, the transformative thesis prevails when globalization is considered politically consequential.

Proponents of the transformative view usually base their conclusions about global governance on one of two arguments. In the first, global governance is considered a *response* necessitated by the supposed disregard for territorial borders by empirical processes of trade, pollution, migration, etc., associated with globalization (Castells, 2000b; Held, 1995, 2004; Held, McGrew, Goldblatt, & Perraton, 1999; Stephen J. Kobrin, 2002). Because globalizing processes can affect individuals in multiple jurisdictions, institutional and policy frameworks

that transcend conventional territorial divisions between political communities are needed (see especially Held, 1995; Held, 2004). The second view, which overlaps with the first, examines the proliferation of non-state actors closely associated with globalization. Because the activities, membership and organizational frameworks of global civil society, transnational corporations, private authorities, amongst others, cannot be circumscribed within the state's territorial borders, they are interpreted as distributing political power amongst a more plural group of actors (Anheiner, Galsius, & Kaldor, 2001; Cutler, Haufler, & Porter, 1999; Hall & Biersteker, 2002b; Rosenau, 2007; Scholte, forthcoming; Tarrow, 2005). The implicit assumption in both of these arguments is that flows, interactions and structures that operate across territorial borders are the "motor behind current trends toward expanded global governance" (Lake qtd. in Cameron & Palan, 2004, p. 31). The visible and growing activity of global governance institutions and practices today is evidence of how globalization's cross-border flows of goods, services and people are creating *global* space as a site of political authority.

As stated, viewing globalization as an objective set of measurable trends tends to focus on sovereignty's manifestation in territorially bounded spaces – hence the emphasis placed on measuring flows that cross territorial borders and the definition of globalization as a process of 'deterritorialization.'[5] Sovereignty has been variably defined in Renaissance, Classical and modern periods (Bartelson, 1995). But the modern, 'inter-national' conception of sovereignty – the idea of mutually exclusive territorial political units – has had the most influence in world politics, the result being that the territorially bordered nature of political

[5] Scholte (2000, p. 16) provides one of the most widely cited formulations of globalization as a process of deterritorialization: "a reconfiguration of geography, so that social space is no longer wholly mapped in terms of territorial places, territorial distances and territorial borders."

identities, communities and authorities has become synonymous with sovereignty (Bartelson, 1995; Ruggie, 1993; Walker, 1993).

However, the theoretical and empirical metrics of sovereignty extend beyond a simple correlation between states' territorial borders and their political authority. Sovereignty is a normative understanding about the location and (by extension) the limits of political and social relations. A number of scholars have shown that this normative understanding is the product of a specific historical constellation of interests, ideas, and material conditions that culminated in discourses legitimating territorially bounded states and their associated institutions as the sites of political governance. This view of the relationship between discourse, legitimacy and authority draws primarily on the work of Michel Foucault (Foucault, 1972, 1977, 1978). Foucault defines discourse – complex historically contingent systems of languages, theories, material practices – as embodying a certain perspective. If political legitimacy can be broadly defined as the "capacity of the system to engender and maintain belief that the (…) political institutions are the most appropriate for the society" (Lipset qtd. in Connolly, 1984, p. 10), a normative justification of a certain arrangement of political authority that garners allegiance, discourse is related to legitimacy because it renders a certain perspective 'normal' and therefore the most appropriate for society. A discursive theory examines how a given vocabulary naturalizes a certain arrangement of political order – in other words, how the appropriateness of various institutions and practices is made to be an obvious 'fact'. Along these lines, the territorial states-system is the outcome of the discursive constitution and inscription of sovereignty as the accepted and expected principle of political legitimacy.

Specifically, as Biersteker and Weber (1996a, p. 3) argue, the discursive legitimation of sovereignty produces the "modern state system … [with] a normative conception that links *authority*, *territory*, *population* (society and nation) and *recognition* in a unique way and in a particular place (the state)" (my emphasis) (c.f. Bartelson, 1995; Biersteker & Weber, 1996a; Ruggie, 1993; Spruyt, 1994). With territory determining the scope of the others, sovereignty has been expressed as the 'territoriality' principle.[6] As territorial borders circumscribe the extent of political power, they give a specific definition to *population*. 'Insiders' are citizens of a particular state; 'outsiders' live in other territorial jurisdictions and are therefore not accorded the same political rights and protection (or, in some cases, exposed to the same kinds of political violence). With borders specifying the limits of political power, *recognition* entails the acceptance by rulers that they cannot intervene, except in limited circumstances, in the governance of other territorially demarcated jurisdictions (Dunne & Wheeler, 2001; Kratochwil, 1995; Vincent, 1974; Weber, 1995). As a result, political *authority* is a matter of controlling the affairs of a subject population of 'citizens' (democratically or otherwise) without the influence of authorities from other states. Taken together, then, sovereignty delimits legitimacy in terms of the inviolability of territorial borders both practically and normatively. Borders ultimately signify the functional jurisdiction of a state, defined by *de jure* principles that sanction it as a space free from the interference of other states or the entry of 'foreign' objects or people.

Illuminating sovereignty's discursive dimensions does not suggest that sovereignty has legitimating power only when states are able to fully control what does and does not cross their borders. Although the speed and volume of cross-boundary flows today is

[6] Territoriality is not simply territory. It is a specific understanding of social geography that links political authority, identity, community, and agency to fixed and mutually exclusive units represented by territorial states (Agnew, 1998; Cox, 1981; Mandaville, 1999; Ruggie, 1993; Sack, 1986; Sassen, 2001; Scholte, 2000).

unprecedented, the trans-territorial movement of goods, resources, and people is not new, and throughout history even the strongest states have been unable to maintain sovereignty in its purest sense. This reinforces and demonstrates the degree to which sovereignty exists through a legitimating discourse: even when evidence suggests that states' borders are more porous than theoretically assumed, sovereignty has remained a powerful and defining force and instituted the state as the locus of domestic and international politics.

When attention is directed to sovereignty's discursive power, then, claims about globalization's transformative impact and its visibility in institutions and practices of global governance must assess not only the way states' territorial borders are passed over – but also whether the phenomenon of globalization offers discourses with principles of political legitimacy that *de*legitimate sovereignty's territorial organization of politics and authorize 'global' space as a site of governance. In other words, if globalization is formulated as the unsettling of sovereignty, deterritorialization must also be a set of discourses that disrupt sovereignty's normative association of *territory*, *population*, *recognition*, and *authority*, the ways these combine to produce and legitimate the particular institutions (i.e. governments, militaries, etc.), and ultimately constitute the spatial organization of politics in territorially bounded states. 'Global' accordingly is and becomes a *political* space when it is defined and constituted as a particular normative framework for political thought and action by discourses of deterritorialization.

It should be stated that shifting the attention to globalization discourses does not devalue the empirical manifestations of contemporary globalization. For instance, the recent and 1990s financial crises demonstrate how the transfer of capital across borders imbricates states in a global, rather than solely national, economic order. Neither does it dispute that

global governance is in part a condition of the way certain dynamics and issues escape the reach and scope of territorially defined political authorities – environmental governance being a classic example. Instead, a study of globalization discourses examines how empirical trends are situated *within* legitimating discourses of global political order – for example, why the movement of capital is tied to neoliberal agendas directed to fostering a global 'market', or how the idea of sustainable development has shaped the understanding of global space as a 'commons', and how both have inspired particular institutional and policy measures.

Others, of course, have attempted to connect the visible empirics of globalization to discursive factors (Cameron & Palan, 2004; Fairclough, 2006; Kornprobst, Pouliot, Shah, & Zaiotti, 2008; Muppidi, 2004; Steger, 2004, 2005). Of particular note are global governmentality scholars (Bartelson, 2006; Larner & Walters, 2004a; Sending & Neumann, 2006). Their work attends to the ways in which globalization terminologies provide "idioms in the exercise of (geo-)political and (geo-)economic power … [that] suggest particular styles and arts of governing" (Larner & Walters, 2004c). But little is said about how and why these *de*legitimate the power of sovereignty.[7] Failing to address the question of sovereignty, investigations into new idioms might show that globalization is a powerful force in political life but its effects may be inconsequential in terms of the meta-narratives and organizing structures of sovereign political order.[8] Within this approach, Hardt and Negri's (2000) discussion of *Empire* arrives at the heart of the normative challenge that globalization poses

[7] Larner and Walters (2004b, p. 2) define global governmentality as "as heading for studies which problematize the constitution, and governance of spaces above, beyond, between and across nation-states." While this takes the focus off the 'domestic' sphere, it does not necessarily say much about how this new space of governance affects sovereignty. In fact, they often use global as a synonym for 'international', suggesting that global governmentality, even if not a domestic rationality of power, can still be rooted in sovereign states.

[8] Sending and Neumann (2006) are a noted exception within this literature. Their argument, however, is not that global governance robs the state of its power but that the logics of power associated with government themselves are changing as non-state actor perform governance functions.

to sovereignty, but their discussion of discursive factors is eclipsed by an emphasis on the expanding scope of capitalist modes of production.

Moreover, studies of global governmentality tend to define globalization exclusively as a discourse of neoliberalism.[9] Although this is one of globalization's most prominent faces, leaving open the possibility that globalization can exist in *multiple* discursive forms allows for an investigation of how 'globalization' (and global governance) can be and has indeed been captured, co-opted, and deployed with vastly different meanings in different contexts – as the contrasting agendas of bodies such as the *World Economic Forum* and their critics in the *World Social Forum* demonstrate. That different – even divergent – meanings can be attributed to globalization makes evident that globalization cannot be discussed in any definitive way. Even if we can speak intelligibly about *global* as a physical or geometric descriptor, its political significance is subject to varying determinations and designations.

A discursive approach to globalization must thereby address a double problematic. First, it must demonstrate globalization's transformation of political order by uncovering *normative* principles that challenge sovereignty and legitimate and authorize global governance institutions and practices. Second, it must develop a typology of global political space that not only accounts for the changing nature of political authority beyond the state and sovereignty, but also, given the multiplicity of discourses of globalization, for how 'global' has been differently shaped as a site of political authority. In the following section, I propose an analytical and theoretical framework for taking on these tasks.

[9] A similar weakness is found in cosmopolitan theories, whereby globalization is considered the pre-condition or the manifestation of (liberal) cosmopolitanism (Shah, 2006). See, for instance, Anheiner, Galsius and Kaldor (2001), Archibugi (2003), Archibugi, Held and Koehler (1998), Beck (1999; , 2005; , 2006), Beitz (1999), Held (1995), Linklater (1998)

Globalization and metaphors

And as Imagination bodies forth
The forms of things unknown, the poet's pen
Turns them to shapes, and gives to airy nothing
A local habitation and a name
~ William Shakespeare, *A Midsummer Night's Dream*, V. 1

A discursive approach to globalization uncovers how globalization has become a 'fact of life' and what kind of 'fact' it represents. It investigates the perspectives that become legitimated, how they define what globalization 'is', and the way this reconstitutes the spatial and institutional organization of politics on a global scale.

The use of metaphors to communicate the implications of globalization provides an opening for investigating the role and significance of globalization's discursive dimensions. Indeed, metaphors are only one feature of discursive structures, and discursive structures themselves are only one element involved creating political societies. However, as described above, metaphors have come to pervade our everyday discussions about globalization and appear to correspond to how the political consequences and responses to 'globalization' are understood. Assessing their specific influence warrants an in-depth exploration and can provide some insight into the way globalization exists and operates discursively.

Metaphors have a long history in Western philosophy and political thought. Broadly, they can be defined as tropes of resemblance between different things and experiences whereby one field is used to describe another. In their most technical definition, metaphors are figures of speech or literary devices used to describe and highlight features of a person or object. There is no shortage of opinion on how to best understand the nature and significance of metaphor in political discourse.[10] Classicists, drawing from Aristotle, argue that metaphors

[10] (Aristotle, 1975, 1982; Beardsley, 1981; Beer & De Landtsheer, 2004; M. Black, 1981; Booth, 1978; Edge, 1974; Goatley, 1997; Hawkes, 1972; Hesse, 1980; Hobbes, 1996; Johnson, 1981; Kittay, 1987; Lakoff &

reflect the 'nature' of political reality by drawing on presumed objective similarities between, say, *villages* and globalization. Postmodernists take their cue from Nietzsche's (1911, p. 180) claim that "truth is but a mobile army of metaphors" and examine how metaphors construct political reality – the metaphor of *villages* constitutes globalization. Underlying these different theories is a view that metaphors *graft* together different fields to produce insights and ideas that have an effect on how political life is perceived. Where they differ – and drastically – is in how perceptions are 'shaped': reflection or constitution.

This turn to metaphors in globalization is not without its critics. Those ascribing to a positivist view of language would argue, following Hobbes and Locke, that metaphors are "absurdities" or "perfect cheats" that obfuscate our ability to properly and rigorously discern globalization's political significance.[11] Although potentially powerful rhetorical devices, metaphors ultimately stand in the way of good social science and therefore must be 'cleared away' in analyses of globalization (Lake, 1999). Marxist approaches make a similar claim: metaphors are ideological and instrumental guises that extend the parochial interests of the capitalist class over the masses (M. Ferguson, 1992). To thwart the ruling classes, we must 'see through' their metaphors, exposing their political projects for what they *really* are.

Others, however, contend that metaphors cannot be so easily dismissed. Sparke (forthcoming), for instance, argues that metaphors "[assume and activate] a distinct imaginative geography of globalization that then frames and visualizes the terrain of [global politics] in a distinct way." Metaphors show that globalization is more than a buzzword but

---

Johnson, 1980; Locke, 1998; Musolff, 2004; Nietzsche, 1911; Nogales, 1999; Plato, 1992; Ricoeur, 1977; Rorty, 1989; Searle, 1981)

[11] For Hobbes, using metaphors was akin to "wandering amongst innumberable absurdities; and their end, contention and sedition, or contempt" (Hobbes, 1996: part 1, chapters 4 and 5). Locke similarly argued in his *Essay concerning human understanding* (1998) that the consequence of metaphor was only to "insinuate wrong ideas, move the passions, [and] thereby mislead the judgement" (Book 3, chapter 10). Therefore however, "laudible or allowable oratory may render them in harangues and popular addresses they are certainly, in all discourses that pretend to inform or instruct, wholly to be avoided" (Book 3, chapter 10).

instead "an influential … discourse about the world." As elaborated on in this study, *global village* inculcates a view of a more harmonious, cosmopolitan society; by contrast, *global war on terror* depicts a global system as a battlefield. As "different metaphors may facilitate or discourage one or the other course of globalization," Scholte (2008, p. x) stresses they "are a significant … aspect of the politics of globalization." Read (2006, p. 1) perhaps goes furthest, claiming that "something about globalization *compels* the production of metaphor" (my emphasis). From his perspective, 'globe' or 'global' are only geometric abstractions. For either to denote a political order, a normative world must be grafted on them. The action of metaphors therefore lies in precisely how globe or global are defined as normative worlds and produced as horizons of political order. Because globalization is a considered a moment of *political* transformation on a *global* scale, investigating such transformations requires interrogating popular metaphors of globalization.

This latter view begs the question of whether metaphors can be 'cleared away' or 'exposed' for masking the 'real' dynamics of globalization. Even if metaphors are mere rhetorical devices, they frame globalization in a particular way. If metaphors of globalization sanction the self-interests of the capitalist class as the interests of society at large, investigating the use of metaphor seems to be a necessary first step in mounting an effective strategy of resistance (c.f. Gill, 1995). Furthermore, given that different metaphors can be – and indeed have been – used to convey what globalization means, it becomes difficult to claim that metaphors reflect an objective process of globalization, or perhaps that globalization itself is a metaphor for accurately describing contemporary processes of political change (Luke, 2004). When the meaning of globalization itself is open to discursive interpretation, it cannot provide an objective point of reference that conveys the nature and

significance of those trends. Whether it is the capitalist class' neoliberal *global market*, the cosmopolitan's *global village* or the security agent's *global war on terror*, it seems that the meaning and significance of globalization is at some level cast by metaphors (c.f. Shah, 2006).

The scales are therefore tipped towards a theory of metaphor that reveals how global is constituted as a political space. In light of the proposition defended here – that without the power to *de*legitimate sovereignty and *re*legitimate political order in some *global* way, globalization is unable to transform political order – attention is specifically focused on the *legitimating* capacity of metaphors, and the ways in which this contributes to the development of spaces of political governance.

Although there are a number of theories in which 'reality' is constructed by metaphors, few address the question of legitimacy (Beardsley, 1981; Bono, 2001; Booth, 1978; Edge, 1974; Goodman, 1981; Nietzsche, 1911; Richards, 1981; Ricoeur, 1977; Rorty, 1991; Searle, 1981). Lakoff and Johnson's (1980; , 1989) widely cited approach, for instance, evades the question because their experiential explanation of metaphors fails to explain how and why metaphors become broader social discourses that condition individuals' perceptions of the world.[12] If applied to the question of political order, this approach would not show why members of a given society collectively accept and endorse specific norms, institutions and practices of political power as the 'most appropriate'.

[12] The main problem with this approach is that while stating that metaphors are broader social and culturally specific narratives, Lakoff and Johnson also contend that metaphors emerge from bodily experiences with the physical world. This experiential account raises questions not only for why and how it is that different metaphors are produced across different cultures (i.e. why do these experiences take on different meanings and representations in different social milieus across space and time?), but further, in light of the argument of this study, how metaphors are socially enforced rather than grounded and derived from personal interactions with one's surroundings.

An alternative approach is found in the work of Richard Rorty (1989). Rorty takes his cue from Nietzsche and considers metaphors as part of the diverse forces that produce broader discursive patterns that constitute social and political life. Combining his understanding of metaphor with Wittgenstein's notion of language games, he shifts the focus of metaphor away from being "criterion-governed sentences" *within* language games to being the broader contexts that shape language games as a whole (Rorty, 1989, p. 5). To the degree that language games provide the sentences by which we talk about the world, 'reality' is a product of the metaphor that prevails in a particular time and place. If political legitimacy has to do with how certain vocabularies define what kind of political governance is 'appropriate', Rorty's approach provides a way to consider metaphor's legitimating power and the role this plays in the formation of political orders.

Rorty defines metaphors as tools by which society can 'redescribe' itself. He contests the view that there is a "single vocabulary" – that is, an objective theory – that describes what political society is or should be. Rather, by understanding that "*languages* are made rather than found" and that as a consequence "truth is a property of linguistic entities, of sentences," we can be open to the possibility of political transformation (Rorty, 1989, p. 7). Political activism, in other words, requires abandoning the position of the *scientific philosopher* – one who seeks to uncover *the* truth 'out there' – and becoming a *poetic one* – one who realizes that "truth is made rather than found" (Rorty, 1989, p. 7). It requires that we "face up to the contingency of the language we use" and realize that history is a matter of "increasingly useful metaphors rather than of an increasing understanding of how things really are" (Rorty, 1989, p. 9).

Understood as *useful* tools, metaphors serve a dual function. On the one hand, Rorty suggests that metaphors are useful because they allow analysts to understand that the 'nature' of the self, of the public sphere, etc. can be described in different ways in order to achieve different purposes. A Galilean vocabulary did not make a discovery about the world but instead "hit upon a tool which happened to work better for certain purposes than any previous tool" (Rorty, 1989, p. 19). Metaphors therefore have a therapeutic purpose. By describing the world in new and different ways, seemingly familiar assumptions look unfamiliar – what is assumed to be natural correspondence emerges as social artefact – and new modes of action and investigation are possible (Deibert, 1997a, p. 182).

But, metaphors do not operate in a vacuum, and so the therapeutic exercise is not only conceptual. Scholars must turn their attention to metaphors because social actors themselves pick up metaphors that they find useful to redescribe themselves and their larger collective projects. As an example, Rorty points to the French Revolution as an instance in which changing the vocabulary of social relations affected a change not only in how human beings thought of themselves (as agents operating autonomously of God's will) but, because of this, of what was considered possible in the social and political societies in which they lived and participated (equal participation by all citizens). Thus, the implication of Rorty's claim that history is a succession of useful metaphors is that analysts view their analytical frameworks as metaphors in order to come to terms with the fact that 'reality' is ultimately a function of human-constructed languages, and because these languages are used by social actors and change over time, that different metaphors are typologies of how social, political and scientific practices have been shaped and how they have evolved over time.

To illustrate how metaphors contribute both to the contingency and construction of human languages, Rorty builds from the work of Donald Davidson (1978). Davidson's pragmatic and performative definition of metaphors disputes the view that metaphorical phrases have special meanings (M. Black, 1979, 1981; Ricoeur, 1977). Along these lines, meaning, for Rorty, is a function of literal language – if a metaphor has 'semantic' power, it ceases to be a metaphor. Rorty argues that because a metaphor is literally speaking a false statement it *disrupts* conventional uses and meanings of existing (literal) language – in other words, according to established standards of language, a metaphor is absurd. This absurdity, however, is not grounds for dismissing metaphors as inconsequential. On the contrary, metaphor's absurdity is a source of creativity. If not producing meanings, metaphors produce 'effects' (non-verbal images or pictures) that generate novel and imaginative possibilities and understandings. For instance, the Shakespearian metaphor 'Juliet is the sun' is literally false (and accordingly absurd). However, *redescribing* Juliet through the 'sun,' the metaphor evokes a new understanding and ascribes to Juliet sun-like qualities, constructing her in a novel way. In this sense, metaphors operate as performative speech-acts, which evoke new insights and understandings (c.f. Davidson, 1978). This notion of description is not about a 'reality' out there that is reflected through metaphors. Rather, description *constructs* images that eventually become so deeply entrenched and habitualized as part of the everyday way of speaking about the world that its metaphorical status is forgotten. When this happens, it ceases to be a metaphor – it is 'dead' – and instead marks a "new stage of literal language" (Hesse, 1987, p. 297). At this point the metaphor's descriptions *define* reality.[13]

[13] Whether Rorty's reading and application of Davidson's philosophy of language is true to Davidson's purposes and objectives is a matter of debate. However, in so far as Rorty develops his own theory of metaphor, his theory can be evaluated (and criticized) independently of its association with Davidson.

Applied specifically to the question of political order, this too is partly constituted by a 'literalized' metaphor. From Rorty's (1989, p. 9) perspective, the suggestion of a particular metaphor at first represents only a potential (an imaginative possibility for political life). However, over time, it "describes lots and lots of things in new ways, until … a new pattern of linguistic behavior [is created]." As these descriptions are entrenched, they become the collective statements about what is 'true' and 'false' to say about a political community. This entrenching in truth establishes the legitimacy of the metaphor's perspective.

The concomitant effect of a new pattern of linguistic behaviour is that it "[tempts] the rising generation to adopt it, thereby causing them to look for appropriate forms of *non-linguistic* behavior, for example, the adoption of … new social institutions" (Rorty, 1989, p. 9) (my emphasis). For instance, in Rorty's example of the French Revolution, the metaphor of the *nation* disrupted assumptions that supported the authority of kings based on divine right. With a new political vocabulary of *liberty* and *equality* that flowed 'naturally' from this new metaphor, parliaments and democratic processes became the new structures and mechanisms of governance (c.f. Näsström, 2003).

This ability of metaphors to shape political order should not take away from Rorty's initial impetus for suggesting that society be studied through metaphors – that is, a metaphor makes political transformation possible. Because of metaphor's 'disruptive' effects and the new possibilities they make imaginable, political orders are created during moments of *metaphorical redescription*: when new metaphors, those that do not conform to established or literalized language games and their associated institutions and practices, are advocated for the adoption of new institutions of authority.

Rorty argues that "[w]hether redescription occurs is a matter of what is going on in the rest of the universe," the historically contingent conditions that trigger the suggestion of a new metaphor, rather than a transcendent historical logic that pushes society closer to the 'truth' (Rorty, 1987, p. 296). Although reality is shaped by metaphors, reality is not reducible to them. Metaphors operate in conjunction with a nexus of different factors that inform the epistemologies by which people understand the world around them – for instance, the cumulative outcome of changes in modes of production, new technological innovations, intended and unintended outcomes of policies, responses to crises or notable events, etc. Metaphors' particular function and significance has to do with the establishment of new language games by which actors come to define 'reality', and how this informs the institutions that are adopted as 'appropriate'. All in all, although Rorty (1989, p. 6) argues that metaphors cause us to have beliefs about the world, they do not and cannot on their own cause beliefs to 'happen.' The analysis of *metaphorical redescription* is therefore not a claim that only metaphors matter in shaping that reality. Rather, it is an empirical question that requires a retrospective analysis and thick description of the contingency and construction of political vocabularies: "random factors which have made some things subjects of conversation for us and others not, have made some projects and not others possible and important" (Rorty, 1989, p. 17).

Because Rorty's discussion of metaphor has been used to advocate a liberal society, commentators have tended to focus more on his defence of liberalism and given only limited attention to his work on metaphor.[14] However, Rorty's non-foundationalist epistemology ultimately roots metaphor in a contingent and non-teleological view of intellectual history: *metaphorical redescription* operates according to a Nietzschean-evolutionary logic in which

[14] Some exceptions can be found in Barnes (1991), Brassett (2008), Calder (2003), Deibert (1997a).

new metaphors, which are new descriptions of political life, kill off others, not for a higher purpose, but blindly (Rorty, 1989, p. 19). Thus, history can move in other directions, making it possible to ascribe to Rorty's theory of metaphor without having to endorse his personal political agenda.

In sum, when political relations in a given social milieu are created *and* transformed through the metaphors used to describe them, political order is not *under* description but produced *through* it. This makes metaphor more than just a literary trope or a heuristic device. Instead, metaphor plays a role in shaping the very reality of political order we expect and experience. Conversely, when metaphors are used to 'redescribe' society, they are tools of political transformation: political actors advocate new metaphors to disrupt an existing language game (and thereby its underlying and accepted metaphor) and encourage the search and adoption of new institutions of political authority. This makes *metaphorical redescription* particularly suited to study of globalization – interrogating metaphors of globalization can reveal not only the potential discursive disruption of sovereignty as the basis of political order, but also how different metaphors of globalization disrupt *each other* and generate different institutions and frameworks – typologies – of global governance.

Specifying the legitimating power of metaphorical descriptions

Rorty's theory suggests that legitimacy emanates as vocabularies render certain perspectives 'factual'. Still, he only intimates the legitimating function of metaphor. Specifically, it is unclear how one moves from the 'imaginative suggestion' of a metaphor by poets to the collective vocabulary of politics, and then the creation of new institutions and practices of

political authority. In order to address the question of globalization's transformative impact, it is necessary to modify and elaborate Rorty's theory in ways that illuminate these dimensions. The revisions and modifications that follow can be grouped into two categories, both relating to the questions of legitimacy and power. The first has to do with how metaphor's language games authorize political institutions. The second has to do with how the political orders engendered by metaphors endure over time. I will address each of these in turn.

1) Non-linguistic behaviours as the 'terminal forms of power'

According to Näsström (2003, p. 819), without grounding emergent orders in a framework of legitimacy, "political decisions would run the risk of appearing arbitrary and illegitimate exercises of power." In other words, for any political order to be authoritative – for its subjects to be inculcated into its system of operation – politics cannot be an artefact of brute force. Authority differs from coercion precisely because it has a claim to legitimacy (c.f. Hall & Biersteker, 2002a, p. 4). If metaphorically defined 'facts' translate into institutions of political *authority*, an account of how metaphors exert power and in turn how that power is legitimated is needed.

There is a close resemblance between Rorty's discussion of metaphors and Foucault's notion of discourse referenced above. Foucault (1977; , 1978) explains discourse's legitimating capacity by referring to the *productive* modalities of power. Rather than assuming that power coerces, Foucault discusses how power constitutes 'knowledge' by instilling a certain perspective and not others as the 'factual' definition of political reality. In this account, legitimacy is an outcome of power – the vaulting of one set of perspectives and

practices to the status of 'fact' specifies what is appropriate – what is 'true' – to know and say about society. Again, authority is conventionally distinguished from (coercive) power because the former is said to have a claim to legitimacy. In this view, legitimacy is an external evaluation of forms of power – such as laws, institutions, etc. However, when legitimacy is established by marginalizing other perspectives as untenable, illogical, irrational, perhaps even reprehensible, power works to legitimate itself. Power is therefore *by definition* authoritative. When metaphors are situated within this theory of discourse and power, a metaphor's ability to establish its perspective as 'fact' authorizes its descriptions of political life.

Drawing attention to this power's productive mechanisms is meant to dispel the view that the formal political institutions (law, government, etc.) are the *sources* of political legitimacy. Foucault (2000) argues that the analytical focus must be on the more mundane practices and techniques that produce a particular idea of what a population of political subjects is and how they should be managed: the focus, in short, must not be on formal bureaucracies as such, but rather on how power operates through decentralized and diffuse networks to impose a certain kind of govern*mentality*. That being said, Foucault does not dismiss the significance of the more formal sites of governance. As Bernstein and Coleman (forthcoming) specify, "[p]olitical legitimacy requires institutionalized authorities (whether concentrated or diffuse)." Foucault in part shifts the attention to decentralized logics of productive power in order to demonstrate that the formal structures (law, parliaments, class, etc.) in a given order become authoritative because they are the products of the knowledge legitimated by particular discourse. He therefore refers to them as the "*terminal* forms of power" – they emerge as a certain perspective is legitimated (1978, pp. 92-93). They are the

outcomes of the way power works discursively to legitimate itself, rather than where legitimate political power originates. Parliaments, for instance, emerged as legitimacy was removed from the context of divine right and redefined within the *nation* metaphor.

While Foucault does not reflect on metaphors as such, there is an obvious compatibility between his discussion of discourse and productive power and the importance Rorty gives to metaphors in shaping political communities. When considered together, the non-linguistic behaviours of a metaphor emerge as institutions of political authority because they are emblematic of a legitimated vocabulary – a set of 'facts' – provided by the metaphor. They are, as Bono (2001, p. 227) puts it, "configured and deployed through the metaphors that are embedded in and operating through them." In assessing their importance and role, the objective is to examine the discursive conditions that produce and sanction them.

It is important to point out that a discursive conception of legitimacy should not detract from the material dimensions of political authority. According to Hansen (2006, p. 22), an examination of the discursive basis of political authority is not intended to "disregard material 'facts' but rather to study how these are produced and prioritized." The materiality of political authority therefore rests in the discursive legitimation of certain resources as 'necessary' for the exercise of political authority – for instance, in Weber's theory of the state, governments have a monopoly over the *legitimacy* to use violence. In short, as power legitimates itself, it delimits its necessary material capacities.

2) <u>Performative speech-acts and the reproduction of political order</u>

Because of its emphasis on political transformation, Rorty's discussion of *redescription* is focused on how to change political order rather than how it endures. But if the importance of metaphors – their 'performative effect' – is to change political order, they must have a lasting effect. Political orders are rarely fleeting but more commonly long lasting environments experienced over the course of different centuries. Metaphors' legitimating power therefore rests not only in their capacity to contribute to the production of political orders but also in their ability to help ensure that those orders are reproduced.

Political orders are dynamic entities. Foucault contends that "discursive practices are not purely and simply ways of producing discourse. They are embodied in technical processes, in institutions, in patterns for general behaviour" (qtd. in Clifford, 2001, p. 98). From the relatively mundane process of voter registration to grand inauguration ceremonies, different tasks perform specific functions that keep the political order up and running. But whether voting is a responsibility or whether a community seeks to valorise its (newly elected?) political leaders rests on that community's understanding of what actions are required and acceptable for the achievement of its political objectives. Seemingly functional tasks are therefore strategic. Even if they appear mundane, the 'logic' of their operation works toward the actualization of specific normative objectives. For instance, registering voters intends to allow for efficacious elections, which ensures a stable liberal-democracy. Power is therefore productive in a very material sense – it shapes and operates through day-to-day activities to install and normalize the perspective promoted by a given discourse as the framework of political authority. In the first instance, undertaking these actions creates the order but, as Butler (1990) has argued, it is their *repeated* and *routine* execution by which power legitimates a certain definition of reality. In her own words, "repetition is at once a

reenactment and reexperiencing of a set of meanings already socially established, and it is the mundane and ritualized form of their legitimation" (Butler, 1990, p. 191). Put differently, power is evident *as* certain practices that are deemed necessary for the successful operation of a given political order. Because they are necessary, they become vehicles by which a particular notion of political legitimacy is stabilized. Thus, their repeated performance not only produces political orders but also reproduces them.

A metaphor is therefore a performative "speech-act" in the dual sense of being a use of language that disrupts but also initiates a set of practices that act out – *perform* – the metaphor's discursive definition ('facts') of political reality (c.f. Butler, 1990). The vocabulary implemented by a metaphor has a regulative function, specifying and empowering certain actions. The repetition of these actions, in turn, regulates which vocabularies remain cogent and normal. Put differently, the practices not only reflect the conditions of legitimacy in a given political order, but as they are repeated over time they entrench that understanding of legitimacy so that the practices are repeated and the political order persists. The legitimating power of a metaphor is accordingly both productive and reproductive; it is made evident through practices by which a political order exists and remains operational over time.

With these elaborations, a metaphor is more than just a figure of speech. It is a discursive practice that constitutes spaces of political order by establishing political legitimacy. Drawing on Foucault, political legitimacy is a relation of power, as a particular perspective is installed as the definition of political reality. It is not based on an individual actor's independent rational determination of an existing rule or institution as acceptable (as in the Weberian account), but more profoundly in how an actor's consent is shaped and

conditioned by the discursive system in which he or she is embedded and how he or she participates in the (re)production of its institutionalized forms of authority.

Along these lines, if political legitimacy refers to what kind of governance relationships should be accepted as appropriate, and if it is a discursive property, it is in part embedded in and by metaphors. As a given metaphor's descriptions become the 'factual' vocabulary of political order, the perspective it promotes – for instance, the equality and liberty advocated by the *nation* metaphor – is translated from an imaginative proposition to the *principle(s)* by which political institutions and practices are created and put into operation. The varying effects (i.e. political orders) of different metaphors also reveal that legitimacy is itself a contingent standard, with its character and community of adherents uniquely defined by different metaphors. In short, the legitimating power of the metaphor is evidenced through its successful 'literalization': the metaphor provides vocabularies that define reality, from which principles of political legitimacy emerge, and as these principles come to the fore, they inform the formation of the requisite practices and institutions of political authority for a given political order. The investigative task is therefore to uncover how this literalization occurs and the conditions that will result in its disruption when a new metaphor is suggested, which is where I will now turn my attention.

Towards a theory of metaphorical reinscription

Elaborating Rorty's theory to draw out the legitimating power of metaphors, the researcher's job is to excavate the underlying metaphors of a given political order and to outline the mechanisms by which those metaphors became entrenched as the 'way to speak' about

political life. This can be detected in several overlapping dimensions, occurring across two different moments. The first moment relates to what metaphors do to help to constitute political orders. It entails the vocabularies that become established, the actions taken to build the political order and then the way both contribute to the institutions and practices that ensure the order's reproduction. These three dimensions can be grouped together as a process *enrolment*. The final dimension of metaphor relates to how metaphors contribute to the disruption of political legitimacy. A metaphor problematizes a set of accepted meanings and practices in order to legitimize its own perspective of political order. This moment can be described as a process of *transformation*. Taken together, *metaphorical redescription* is a somewhat misleading label of how metaphors operate. The productive and reproductive logics of governance institutions and practices reveal that a metaphor's legitimating power rests in how it is continually *inscribed* as the framework for political thought and action. The disruptive logic of metaphors therefore reveals how a given inscription is 'effaced' by a new one. The work of metaphors in shaping political orders is therefore more accurately illuminated *as* a process of *metaphorical* ***reinscription*****,** which operates through successive moments of *enrolment* and *transformation*.

Recalling that metaphors operate within a constellation of other factors – and that whether new metaphors emerge is a somewhat random effect of how events, actors' behaviours, productive structures and institutional choices, amongst others, in a particular time and place interact and influence each other – it is important to keep in mind that *metaphorical reinscription* does not 'drive' the construction of political order. As Rorty says, other contextual features 'trigger' the suggestion of a metaphor. The 'literalization' of

metaphors must be understood as one element contributing the creation and transformation of political orders – specifically, through its delineation of political legitimacy.

Metaphorical reinscription therefore pinpoints and illuminates the unique contributions and constitutive influences of metaphors in the construction (and deconstruction) of political orders. Subsequent chapters in this study will undertake a textured investigation that relates metaphors to the specific events, people and material conditions that 'trigger' their suggestion and adoption and how this literalization is consequential in their development of specific governance institutions and practices. Given the dual 'use' of metaphors as tools, *metaphorical reinscription* is a way both to provide an alternative analytical and theoretical method for evaluating political events and processes – in this case, globalization – and also a way to investigate how metaphors become alternative tools for social actors and do the work of generating new vocabularies and institutions. In this way, it is a framework for both assessing events and actions in a particular time and place through the lens of a given metaphor and also for understanding how those events and actions are manifestations of that same metaphor.

1) Enrolment

If governance can be generally understood as the attitudes, policies, institutions and procedures that build and maintain a political order, metaphors matter because they can shape governance structures so that they promote and achieve certain desired objectives. Because the legitimacy, and thereby the relative stability, of any given order requires the allegiance of its members, inscription largely relates to how the legitimating power of the metaphor enrols actors with diverse, even divergent, interests to support these objectives (c.f. Latour, 1987).

i) Political Vocabularies

The most obvious dimension of enrolment relates to the incorporation of a metaphor's descriptions as the *political vocabulary*, which defines the 'facts' of a political order. This is not based on a blind acceptance of metaphorical descriptions. According to Latour (1987, p. 42), 'facts' emerge as a "rather late outcome" of a series of controversial debates and negotiations whereby some actors persuade others that a certain set of descriptions are the most useful for describing society (c.f. Rorty, 1989, p. 9). The strength of metaphorical descriptions therefore relies on the way they are deployed as *the* way to speak about political order by being incorporated into the shared 'oeuvre' of society, which includes scholarly texts and theories, popular press, laws, constitutions, and even literary works. Incorporation of a metaphor's descriptions in other words constitutes a community's collectively held knowledge about political order (Latour, 1987, p. 42). Widely cited theories of globalization, in this sense, even if they derive from an objectivist or empiricist standpoint, reinforce a narrative of globalization (Cameron and Palan 2004).

According to Edge (1974, p. 137), once a metaphor is embedded, its metaphorical status is forgotten as those operating within its descriptions " 'take [the metaphor] seriously' and proceed 'to spell out' their new perception in direct detail, [imposing] the categories determined by metaphor" (c.f. Bono, 2001). In this way, the metaphor's vocabulary provides the "terms … in which decisions must be calculated and justified" (Rose & Miller, 1992, p. 184). Thus one way of detecting how a political vocabulary establishes certain 'facts' is to identify the answers to questions about *why governance occurs*, *what is governed*, *who governs*, *where governance occurs*, and *how governance occurs*, which specify how a

political order must be constructed and managed. Even if the metaphor fades from view – that is, becomes literalized and circulates only through its vocabulary – its incorporation is visible in the emergent answers to the 'why,' 'what,' 'who,' 'how,' and 'where' of governance.

ii) Networks of Action

The second dimension of *metaphorical reinscription* refers to the formation of *networks of action* – the diverse activities that do the practical work of creating a political order. Convergence around a political vocabulary and its specified sets of 'facts' creates debates about what activities are needed for implementing the political objectives endorsed when a specific metaphor is advocated. The establishment of a vocabulary also relies on actors accepting that it is in their interest to do the practical *work* needed to support a given set of political goals. Miller and Rose (1990) argue that to garner this acceptance, strategies of persuasion, intrigue, calculation, and rhetoric are used by some actors in order to convince others that what appear to be conflicting interests actually overlap. This process of 'recruitment' results in the "construction of allied interests. … [It] assembles actors together into a network not because of legal or institutional ties or dependencies, but because they have come to construe their problems in allied ways and their fate as in some way bound up with one another" (Miller & Rose, 1990, p. 10).

Because *networks of action* are formed through the strategic ability of some actors to convince more and more people and things to adopt specific interests, the formation of networks reveals how the legitimation of 'facts' relies on marginalizing other perspectives. If those with different interests are not recruited, either because there is no overlap between

positions or because certain groups refuse (or both), they are pushed to the sidelines. These marginalized groups will either in time succumb and join the network or form sites of resistance (Foucault, 1978, p. 100). With one set of interests empowered over others, *networks of action* reveal that enrolment is an asymmetrical process (Latour, 1987).

Recruitment enables *networks* of action because different actors' participation and conformity with the emerging political order will vary. Recruitment works by redirecting actors' interests and identities, defining for them specific roles and responsibilities that buttress the political order's specific goals. Actors will therefore continue to participate in the political order from their local environments, and often with very provincial agendas. But their aggregate effect constitutes and stabilizes the order because each activity at some level supports the order's objectives..

At some point many of the network's activities become consolidated into more formalized and centralized structures of authority. Actors may pursue such formalization at the outset of a new vocabulary's suggestion (as the discussion of ICANN in chapter 2 will show) or it may be an unintended consequence that develops gradually (as the redefined roles of ISPs suggest in chapter 3). This formalization and centralization does not refer to an organization that directs or supervises every activity in the political order. It may emerge as a node within the broader network, performing a specific function that requires a more consolidated approach to ensure that political objectives are met. It is when this consolidation occurs that formal governance institutions – non-linguistic behaviours – emerge and assume prominent roles in a given political order.[15]

[15] Institutions do not need to be 'formal' to be governance institutions. The operation of norms in society, for instance, may occur informally but still have governance effects in terms of enforcing political objectives and creating political order (Kratochwil, 1991; Onuf, 1989). But all political orders, even if their primary governance modalities exist at the level of decentralized networks, have some kind of public and formal

The 'localized' roles and responsibilities of different actors in the network do not necessarily end with consolidation. Rather, they can be responsible for the operation of the institution or support it in some way. For instance, liberal democracies may root political authority and governance in parliaments, but activities of MPs, their constituency offices, pages, sergeants at arms, and a whole range of less prominent personnel all have habitualized roles that, even if partial, are required for the parliament to have its amalgamated form in the public sphere. The public prominence of a governance institution makes it a 'black box', eclipsing the network from which it emerges (c.f. Latour, 1987, p. 131). Particular kinds of institutions are therefore visible 'evidence' of a given political order because people begin to speak of governance in terms of formal structures rather than the dispersed activities of different groups. This partly explains the emphasis placed on global governance institutions as indicative of globalization's transformation of political order.

iii) Performance

The third dimension of enrolment entails the ratification of legitimating principles through the *performance* of governance practices. As formal institutions eclipse networks, institutions appear to move with their own momentum. The terms of reference established by a political vocabulary therefore create a discursive space that not only influences the roles and responsibilities produced in *networks of action*, but also delineate certain institutional practices that ensure the continued inscription of the metaphor and the reproduction of the political order.

---

institutionalized form. An investigation of metaphors helps to show how these formalized structures emerge with specific governance functions as a result of the inscription of a given metaphor as the legitimating principle of political order.

Constitutions, bills, operational procedures, standing rules, amongst others, are the reference texts or 'operational manuals' of governance institutions. As part of the oeuvre of society, the tasks they outline reflect the entrenchment of a certain metaphor's political vocabulary. To reiterate, the prescriptive nature of these practices is partly functional – that is, if there are no elections, there will be no representatives to debate in parliament and make decisions – but also strategic. Through the regular enactment of elections and open debate, equality and liberty are established as the 'foundational' principles of political life. Once liberty and equality are the assumed political goals, they reinforce the importance of parliaments in maintaining this kind of 'legitimate' political order. Said differently, as governance practices are performed, their 'performative logic' sanctions specific governance institutions as the sites of political legitimacy and authority and their practices become routine and expected features of governance. Parliaments therefore are the public emblems of a liberal democratic political order because they are the operational sites through which liberty and equality are promoted and protected.

The performative significance of a metaphor therefore in part relates to how governance practices construct political orders by evoking the 'facts' of the metaphor - both at the level of political discourse (what are the *answers* to the 'why', 'what', 'who', etc.) and also in their institutionalized form in formal organizations and procedures (what *are* the 'why', 'what', 'who', etc.). To the degree that evoking 'facts' robs the metaphor of its imaginative disruption, it reflects only that the metaphor has become the basis of political legitimacy. To make the point as clearly as possible, metaphors achieve their constitutive effects when a set of governance routines are repeatedly executed such that its perspective is

continually inscribed as the legitimating principle of political order. Repetition, as Butler says, is the course of legitimation.

Through performance, the metaphor's inscription through enrolment comes full circle: the literalization of the metaphor as the legitimating principle of political order is the result of the incorporation of *political vocabularies* and the recruitment of actors into *networks of action* that generate governance institutions and practices. In turn, the repeated *performance* of those practices normalizes the legitimating principle inscribed by the metaphor. This sanctions those governance institutions as sites of legitimacy, which ensures that these practices are repeated and that the political order is reproduced. All of this reinforces the normative tenor of the metaphor as the definition of political 'reality.' Governance, as a result, is not just the outcome of metaphorical inscription in the form of attitudes, institutions and practices – it emerges as inscription's and enrolment's operational impulse, a process by which political spaces are created through both the production and performance of 'facts'.

In sum, although the inscription of metaphors is ultimately contingent on complex and seemingly disparate historical factors, when they coalesce, metaphors contribute to the formation of new political spaces as their legitimating power enrols actors into new patterns of governance.

2) <u>Transformation</u>

Because in the first instance a metaphor is absurd, unsettling the literalized work of a previous metaphor by using language in unintended and unprecedented ways, Rorty (1991, p. 163) attributes to metaphor a transformative power, one that makes it possible to change

"ourselves and our patterns of action." Metaphor's performative effect therefore matters in the first instance as an attempt at political transformation.

Because metaphors ultimately constitute political orders through the repeated *performance* of governance routines, the disruptive effect of a new metaphor rests in its capacity to *misappropriate* governance practices. As Rorty (1989, p. 16) puts it, "Old metaphors are constantly dying off into literalness, and then serving as a platform or foil for new metaphors." Butler (1990, pp. 198-199) argues that in any given order, no matter how stable its routines appear, there is always a "possibility of variation on the repetition," which turns governing practices against themselves and "spawns unexpected permutations." The disconnect between the routines and the legitimating principles to which they correspond can, as a result, undermine the legitimacy of the existing order itself and call the order into question (Connolly, 1984; Habermas, 1973). In short, by creating uncertainty about the 'facts,' misappropriation of governance practices triggers a 'legitimacy crisis'. The palatability of a vocabulary is put into doubt, creating insecurities about the efficacy and desirability of the actions and institutions by which a political community operates and identifies itself.

Again, there is no definitive set of factors that can predict when a metaphor will effectively dislodge the legitimating power of a previous inscription – that is, the historical context and facts that trigger the suggestion of a metaphor are unique to time and place. What can bring about legitimacy crises are the contingent and arbitrary forces of history (Näsström, 2003). These forces can include a concerted effort by individual actors to resist the authority of an existing order, the unexpected consequences of governance programs and policies, or

even disasters and sudden and unexpected events. In each case, the conditions are established for a new way to describe political reality.

Given that the ultimate effect of suggesting a new metaphor is to constitute a new political order – to reinscribe by redescribing, at what point does disruption move to production, from delegitimation to legitimation? How, in short, is the crisis resolved? Metaphors' problematization of the order results from the suggested reformulation of political ideals – a new imaginative vocabulary – and institutions. The discursive force of a new metaphor's descriptions therefore "[catalyzes] previously existing actors, things and temporalities, or spatialities into a new manner and procedures and instantiates new capacities" (Rabinow qtd. in Mackenzie, 2005, p. 388). A new metaphor's disruptive effect is therefore visible only as and when a new process of enrolment is made possible: by proposing an alternate principle of legitimacy and working to reconstruct the political field by incorporating new facts, recruiting people into new networks of action, and ratifying this new order by implementing new governance routines. Disruption is therefore not synonymous with destruction – discontinuation of one inscription process simultaneously initiates another. Political change may be initiated by the disruption of regulatory practices, but its delegitimation of an existing order is a moment of metaphorical *re*inscription through which new metaphors emerge to legitimate and establish different political orders.

It is important to note that delegitimating previous metaphors will not necessarily lead them to disappear, as they may instead be displaced into subordinate, marginal, or peripheral positions of power. They may even mutate and incorporate the perspective of the new metaphor, reinforcing the order it seeks to create. Studying *metaphorical reinscription* is therefore a question of assessing the *relative* power of different metaphors at particular

moments and accounting for their prominence, mutation or marginalization. This also provides further insight into the conditions for political transformation. Metaphors put in peripheral positions of power can become resistance narratives by being redrawn and invoked in different ways to question the legitimacy of newly inscribed metaphors, imbuing them with the potential to disrupt and initiate new inscriptive projects.

Enrolment and *transformation* are two-sides of the 'inscriptive' coin. Studying one requires attending to the mechanisms of the other – indeed, neither would be possible if the other did not take place. When the two dimensions are married, the methodological task becomes clear: an investigation of the historically contingent events, actors and conditions – Rorty's 'random factors' – that create moments of crises and galvanise the adoption of new political vocabularies and institutions. These two dimensions of *metaphorical reinscription* inform the analytical framework used in the chapters that follow. The three empirical chapters, each devoted to one of the metaphors under investigation, are comprised of seven sections

- the first section provides an overview of the historical context that leads to the suggestion of a metaphor of globalization and outlines the metaphor's normative 'features' as they relate to the Internet;
- the second section discusses the use of the metaphor to disrupt 'sovereign' patterns of Internet governance. It examines how existing governance practices are undermined or transformed and describes how this results in a legitimacy crisis;
- the third section describes the adoption of the metaphor, examining the debates through which a metaphor's descriptions become a political vocabulary. It delineates how the vocabulary legitimates a certain perspective and defines the terms of reference – or the 'facts' – for governance. In short, it evaluates how the adoption of the metaphor establishes a new principle of political legitimacy;
- the fourth section discusses the recruitment of diverse actors and the *networks of action*. It first identifies how different actors take on new roles and responsibilities as the political vocabulary gains prominence, and links these roles to the normative perspective

of the metaphor. It then describes how these seemingly disparate activities become consolidated in governance institutions;

- the fifth section examines the development of governance practices. It considers how certain practices become prescriptive such that their repeated *performance* facilitates the endorsement of legitimating principles over time;

- the sixth section considers the effects of 'asymmetrical enrolment', describing how alternative metaphors (of sovereignty and globalization) and their supporters are put in subordinate positions;

- the final section evaluates the role of metaphors against alternative explanations for each of the governance structures discussed. It describes how the investigation of metaphors either overcomes the shortcomings of contending approaches or compliments their analyses.

Investigating globalization as global governance

Having made these elaborations to Rorty's discussion of metaphor, I can now better reflect upon the implications of conceptualizing globalization discursively, and delineate the central problematique of this study.

I have argued that if globalization is to be transformative, it must provide normative discourses of deterritorialization that reformulate the principles of political legitimacy, such that *global* governance structures become necessary and embedded in political thought and action. The connection between globalization's concrete manifestations – empirical flows, institutional structures, and so on – and the discourses that surround them rests in how these 'visible empirics' of globalization are both discursive 'effects' and modalities through which new principles of legitimacy become inscribed. Assessing globalization requires uncovering these discourses, considering their disruptive effects for sovereignty. Moreover, in light of the different images, rhetorics and narratives of globalization, the circumstances that have

inscribed different normative meanings to 'globalization' in different contexts must be identified and elucidated.

This task can be attempted, I have said, by taking a cue from metaphors of globalization. Without attempting to reduce globalization to the play and flux of metaphors, I contend that the prominence of certain metaphors in scholarly, policy and popular discussions of globalization warrants an exploration of metaphors' specific influence on understandings and practices of 'global' politics. Metaphors, I suggest, illuminate one way in which globalization works discursively. My argument is not that globalization only works discursively but that it must at some level work discursively if we are to both investigate and conclude that has it has transformed political order. Specifically, then, my hope is that by drawing attention to metaphors, and illuminating globalization's discursive dimensions through them, we can overcome the shortcomings in interpreting globalization as an objective set of forces and consider how it works normatively to legitimate global governance.

With this in objective in mind, I draw from Rorty and present metaphors as a pragmatic hypothesis. I first suggest metaphors as a therapeutic exercise. By redescribing globalization through the lens of metaphors, I hope to show that globalization can be investigated and conceptualized discursively – metaphors, in other words, provide an alternative analytical tool for illuminating the processes by which principles of political legitimacy are defined and accepted. However, because globalization is conceptualized discursively, it also means that we must attend to the way that globalization is open to different discursive interpretations, not just by analysts but also by social actors. I therefore also suggest metaphors are tools by which actors have come to redefine and reconstruct the

normative basis of political order. Metaphors therefore attend to the double problematic of a discursive theory of globalization by 1) uncovering how it operates normatively, and whether this represents a challenge to sovereignty, and 2) because different metaphors circulate, the metaphors provide a typology of global governance that analysts can use to investigate and uncover the discursive shifts that have affected the legitimation and production of global governance institutions and practices in different contexts over time.

Developing a theory of *metaphorical reinscription,* the implication is that the production of global political space occurs in part through the progressive 'literalization' of metaphors of globalization in and through governance institutions and their procedures. Understanding the influence of metaphors in this way, the claim that the rise of global governance institutions and practices is evidence of global transformation therefore might not be completely off the mark. If processes of *metaphorical reinscription* deploy political vocabularies that 'inspire' institutions, the visible activity of global governance institutions could be indicative of how globalization has affected a change of political legitimacy.

But if globalization is understood in this way, the relationship between globalization and global governance institutions and practices must be reformulated. Global governance must be studied as more than a *response* to the empirical challenges of globalization, because without attending to discursive forces it is not clear how globalization (and global governance) provides a reasonable challenge to sovereignty and its associated state-centric modes of governance. Certainly, interpreting global governance dynamics as embedded in the empirics of globalization - i.e. the actions of non-state actors – goes some way to rectify this gap. However, tabulating the number and type of non-state actors that exist says little about how these actors have been accorded a form of *legitimate authority* (c.f. Hall &

Biersteker, 2002a, pp. 4-5). Furthermore, it is not enough to point only to the terminologies of globalization as the idioms of power as global governmentality scholars do. If globalization's transformative impact manifests in global governance institutions and their policies and practices, it is necessary to uncover how these terminologies become institutionalized in formal sites and practices that reinforce and extend their meaning.

All in all, if globalization's transformation of political order is evidenced by the emergence of global governance institutions and practices, globalization must be seen a legitimating discourse that operates in part through metaphors to produce global governance institutions. Moreover, through their practices, global governance institutions themselves embed these metaphors as the frameworks of political legitimacy. Globalization, in other words, *would be* global governance – the production and performance of 'facts' that sanction and reproduce a deterritorialized 'global' political order.

Investigating globalization *as* global governance is the animating problematique of my foray into globalization discourses through the pragmatic hypothesis of metaphors. Through the case of global Internet governance, the remaining chapters in this study are structured around investigating how global political spaces have been constructed through the legitimation of different kinds of global governance institutions and practices. They explore how institutions and practices considered to be manifestations of global governance are in part products of and instruments through which metaphors of globalization have challenged sovereignty and created structures of political order. Overall, the dissertation examines the degree to which metaphors of globalization have played a role in creating globalization as a legitimating discourse of global governance, and to this end whether and what kind of global governance institutions and practices become the means by which

globalization discourses are upheld as the 'factual' narratives of political reality. Furthermore, the identification of different metaphors examines how and why globalization can be co-opted to promote different political objectives. The investigation therefore not only inquires into the consequences for sovereignty but also the relative power of metaphors of globalization against each other.

An important qualification must be made. This investigation begins with the premise that globalization is indeed an important political phenomenon, and that global governance is increasingly a facet of everyday political reality. References to globalization's opportunities and constraints by policy makers and popular pundits, the prominence of institutions such as the World Trade Organization, and the power of private authorities suggest that globalization has informed political agendas and resulted in forms of global governance. At the same time, I acknowledge that these developments are only the cusp of a historical process whose full implications will only be manifest after several decades, perhaps centuries. Global governance institutions remain relatively underdeveloped as compared to the formalized bureaucracies of the sovereign state. I therefore do not claim that sovereignty and the state are defunct. I attempt to address through a familiar example of globalization – the Internet – the preliminary ways in which sovereignty is being fractured, and the instances in which this is giving way to novel forms of global political legitimacy, power and authority. A limitation of my approach is therefore that it does not provide a way to theorize the temporal dimension of transformation – that reinscription occurs in different stages over the course of decades, perhaps centuries.

Inscribing sovereignty: the *state of nature* metaphor

Studied through the lens of *metaphorical reinscription*, the possible delegitimation of sovereignty must be explored as a disruption of its constitutive metaphors. Although an extended analysis of the conditions that led to the introduction and eventual inscription of these earlier metaphors is not the focus of my investigation, a brief summary of the political order legitimated and visibly inscribed provides a background for understanding how and why sovereignty is challenged by the metaphors of globalization.

Again, the emergence of the modern sovereign states-system cannot be understood purely as a product of metaphors. The sovereign state emerged as a result of a confluence of different and independent trajectories of development from diverse areas in medieval life. This convergence culminated in a crisis of legitimacy regarding the existing system of political rule (the feudal order and its 'Great Chain of Being' metaphors) and triggered demands for new descriptions – new metaphors – of political community and authority (Deibert, 1997b; Murphy, 1996; Ruggie, 1993; Sims & Walker, 2003; Spruyt, 1994).

Of these new descriptions of political order, the *state is a person* and the *state of nature* emerged as central motifs. In particular, their articulation in Hobbes's (1996) *Leviathan* marked a watershed development (Skinner, 1989).[16,17] Assuming first a *state of*

[16] Although Hobbes's metaphor has antecedents in a broader 'body politic' imagery that can be traced back to Plato and Aristotle, and more directly to its circulation in political and legal texts in the early medieval period (Kantorowicz, 1957; Nederman & Forhan, 1993), he did not employ the metaphor in the same way. He neither justified a particular political rule based on its 'organic' affinity with nature (specifically, the human body) nor did he authorize the ultimate and divine authority of the king by equating the kingdom (body politic) with the body of the king. Instead, Hobbes introduced the idea of the 'state' as an abstract political *individual* that existed independently of rulers and the ruled.

[17] Hale (1971) argues that Hobbes's discussion of the social contract actually signals the end of the body politic metaphor in political theory. However, although Hobbes moves away from the ancient and medieval articulations of the metaphor, he does not completely abandon it. Instead, he transforms and resituates it in a different historical context (see Rasmussen & Brown, 2005).

nature between sovereign and thereby autonomous individuals,[18] Hobbes argues that in the absence of an overarching authority, the autonomy of individuals is a source of insecurity: in the state of nature equal entitlements to security result in the constant possibility of war. For the sake of their security individuals transfer their autonomy to the Leviathan. By transferring their autonomy, the state is individuated, vitalized by its sovereignty: The 'great LEVIATHAN called a COMMON-WEALTH, or STATE, (in latine *CIVITAS*),' asserts Hobbes (1996, p. 9), 'is but an Artificiall Man; […] and in which, the *Sovereignty* is an Artificiall *Soul*, as giving life and motion to the whole body.' Like individuals the state exists in a *state of nature* with other states, as the autonomy-*cum*-sovereignty at the core of the 'state is a man' metaphor gives way – or perhaps reverts – to a corporatized version of the *state of nature* metaphor – i.e. a *state of nature* between states in which every state exists in a perpetual 'security dilemma', facing the constant threat of war from other states. As Hobbes (1996, p. 90) puts it, men, 'because of their Independency, are in continuall jealousies, and in the state and posture of Gladiators; … which is a posture of War.'[19] Hobbes, however, does not advocate a global Leviathan[20] because, in his view, states maintain their autonomy and are responsible for their own security against one another.

Within this rendering of political life are the basic elements of international relations theory and practice: because states have been made into 'people', their 'anarchic' relations occur in a state of nature. Because of the pervasive security dilemma, the 'insider'/'outsider' distinction becomes a metric of security – 'insiders' or citizens are 'friends', while

[18] Kirby (qtd. in Cameron & Palan, 2004, p. 64) argues that in the Enlightenment, the individual was understood as "undivided within itself, and unquestionably separate from other subjects and the external environment as a whole" — in other words, the individual was a sovereign and autonomous being.
[19] See also Ringmar (1996) and 'Forum on the state as a person' in *Review of International Studies* (2004), 30(2).
[20] Although Hobbes does point out that the *state of nature* between states is hardly as pernicious as the *state of nature* between individuals, it still remains a conflict-ridden – hence, his description of states as 'gladiators' (Hobbes, 1996, p. 90).

'outsiders' or foreigners are 'enemies' (Walker, 1993). Sovereignty – the "soul" of the state and the expression of its community's autonomy – becomes the foremost legitimating condition in a world defined by territorial states.[21] While Hobbes does not discuss the sanctity of territorial borders as a signature feature of political sovereignty as such, the influence of his metaphors towards this development is incontrovertible. Only if states are defined as sovereign (inviolable) persons would their borders be upheld as sacrosanct. Only if states are defined as sovereign (inviolable) persons would they have the authority to solely govern their own affairs, and thus rightly defend against the potential intrusion of others. The anthropomorphizing of the state translates into assumptions about the indivisibility of sovereign authority over the territory of the state.

Certainly, Hobbes was not the only political commentator to employ the *state of nature/state is a person* metaphor (c.f. Kantorowicz, 1957; Rasmussen & Brown, 2005; Sims & Walker, 2003). As Bartelson (1995) argues, understanding sovereignty as a discourse requires recognizing that sovereignty does not have a definitive or fixed definition but that its meaning is open ended. But even from different perspectives, the *state is a person* metaphor has informed the ontological status of the state and in turn has informed the depiction of the international system as a *state of nature* in which territorial integrity is the focus of political legitimacy (Ringmar, 1996).[22]

[21] It is important to note that Hobbes doesn't use metaphors strategically or consciously. Based on his positivist view of language, Hobbes deplores the use metaphors. However, his political vocabulary is thoroughly embedded in a specific set of metaphors, which say little about the reality of political life in an objective sense but in the historical context he is situated, they had become seminal parts of an evolving discourse about statehood (Skinner, 1989). This adds greater support to the discursive theory of metaphor and provides evidence of metaphors' normative dimension. Even more, that Hobbes employs them so unproblematically and does so while dismissing metaphor demonstrates how metaphors become literalized into vocabularies that define the 'facts' of political life.

[22] Others, specifically Locke (1988) and Kant (1996), also employed these metaphors, albeit without the same pessimism as Hobbes. This demonstrates the degree to which a particular metaphorical description of political life came to define, describe, and determine political life both within and between states. While there are

Metaphors of globalization can disrupt the naturalized practices and assumptions in the *state of nature* metaphor by putting its legitimacy into 'crisis.' Because the tenor of political 'crisis' for the state is a common theme in discussions of globalization (Bernstein, 2004; Bernstein & Coleman, forthcoming; Held, 1995; Steffek, 2003), an important part of investigating the transformative effects of globalization is to identify the metaphors that accompany this sentiment and the way in which they may be calling the *state of nature* metaphor into question.

Making sovereignty and the *state is a person* and *state of nature* the frame of reference for metaphorical disruption in the context of globalization is not meant to demonstrate that globalization represents a single legitimating discourse expressed through different metaphors. This study examines a number of different metaphors of globalization – such as *global village*, *global marketplace* and *global war on terror* – and finds that they proffer varying legitimating frameworks, and so construct different global political orders. As will be shown, different metaphors provide differing analyses of how sovereignty as the standard of legitimacy is thrown into crisis by globalization, and subsequently differ on the principles that legitimate global political order. Their divergent interpretations make evident that neither globalization nor sovereignty can be discussed in any definitive way.

Metaphors of globalization and global Internet governance

---

notable differences between the various applications of the metaphor between different authors, the differences amount only to different accounts of the *state of nature* and the nature of the individuated state rather than different metaphorical renderings of political community. As Alexander Wendt (1999) has indirectly demonstrated, Hobbesian, Lockean, and Kantian applications of the metaphors are all rooted in the principle of sovereignty; they represent different logics of international anarchy rather than alternative units of political community or arrangements of political authority.

I investigate three metaphors in this study – *global village*, *global marketplace* and *global war on terror* – and explore their consequences for constructing global political orders and the institutions and practices of global governance. As a prelude to the discussion that follows in subsequent chapters, it is worth briefly reflecting on each metaphor of globalization and their association with the Internet.

The *global village* prompts images of a peaceful world community. This traces back to the anti-war movements of the late 1950s and 1960s. The legitimating ethos entailed here, I will show, has to do with 'openness' – creating a world polity, a village on a global scale – that includes all members of humanity. It delegitimates sovereignty because of sovereignty's propensity to create war by dividing humanity into 'national' communities. Governance along these lines is directed at creating either more dialogue between international leaders, the idea of a world government, and most popularly through grassroots, direct and deliberative democracy, today associated with a putative 'global civil society'.

The *global village*'s popularity as a metaphor of globalization has in part continued because of the popularization of the Internet as a communications medium that transcends national and cultural boundaries. However, rather than assuming that the Internet naturally gives way to the non-sovereign, globalized communities, I will show that this was actually a result of how the metaphor's articulation in the countercultural movement promoted cosmopolitan and cyberlibertarian visions for a new kind of cyberspatially structured global order and converged with the interests of certain computer science communities. Exploring these developments through the pragmatic lens of the *global village* metaphor, 'openness' was translated as 'open access', promoting planetary, decentralized, bottom-up practices for technical standards development. Although the metaphor became institutionalized in many

ways, one prominent example of the metaphor's consolidation into concrete governance institutions and practices was the creation of the *Internet Engineering Task Force* (IETF) and its 'Internet Standards Process'.

The *global marketplace* metaphor has a more recent history, tied to promotion of neo-liberalism. Beginning in the 1970s, the popularity of neoliberalism reached its apogee in the late 1990s, and in many circles continues to be policy orthodoxy. Presenting transboundary economic flows as unavoidable, sovereignty, expressed through government regulation, is considered detrimental to economic prosperity. Deregulation is considered necessary for effective 'competition', the latter of which subsequently emerged as a legitimating principle for a number of policy objectives. Under this metaphor, 'global' governance is a matter of diminishing state power and enhancing private authorities. Today the global marketplace appears to refer to an actually existing entity rather than a metaphor. I will show that this 'literalization' occurred because neoliberal ideologies successfully translated the 'market' into a global imaginary and redefined globalization as a capitalist economic phenomenon (c.f. Steger, 2005).

The Internet was heralded by political leaders and business leaders as "the" platform that would make the global marketplace a reality. Although the motif of the *global marketplace* metaphor in Internet governance can be assessed along many dimensions, it had a particularly prominent effect on the distribution of domain names. This story revolves around the creation of the *Internet Corporation for Assigned Names and Numbers* (ICANN), a private authority mandated with creating a competitive and global domain name market, which, it was hoped, would ensure that the global market more generally was a competitive space.

In the aftermath of the terrorist attacks of 11 September 2001, the *global war on terror* has generated a new discourse of globalization. The threat posed by transnational terrorist networks has moved the topography of war to a global context. In contrast to the peaceful and profitable potentials inscribed into global space by the *global village* and *global marketplace* metaphors respectively, under this new metaphor globalization emerges as a pernicious force with a 'dark side' – global space is defined as a war zone. Rather than solely referring to the protection of states, the new conflict is also described as a war between 'global civilization' and 'global networks of terror.' These developments have not pushed aside the importance of national security and the protection of the state – on the contrary, they continue to matter very much. But to the degree that the metaphor redefines the categories and referents of war on a global scale, the metaphor promotes global 'security' as a legitimating framework for global governance.

Because terrorists use the Internet to organize and recruit, governments, law enforcement and intelligence agencies have come to view the Internet as a "terrorist's safe-haven" and thereby a central front in the fight against terrorism (Schmitt & Shanker, 2008). Although the heightened security context has resulted in policies that to some degree 'reterritorialize' the Internet, terrorist use has complicated the ability to identify and locate threats on the basis of distinguishing between 'citizens' and 'foreigners'. This has created tensions for governing the Internet according to principles of national security and has generated practices that reflect a continuation of the Internet's global governance under a 'global security' principle. The specific effects of the metaphor, I argue, are evident in the expansion of government powers of surveillance and censorship. Because Internet Service Providers (ISPs) provide access to the Internet they have become the institutional centres of

this effort. Because of the way their surveillance and censorship roles and responsibilities are articulated within and shaped by the discursive context of the *global war on terror* metaphor and its 'global security' principle, increased government control of ISPs is not automatically evidence of sovereignty.

Evidently, the normative direction and tenor of the Internet's globalization has been variably defined not only vis-à-vis sovereignty but also with respect to the Internet's purported global political potential and character. Exploring the events and processes through which these definitions have been inscribed, and why they have changed over time, can shed light on globalization's discursive power and its influence on governance structures.

Still, the Internet's relation to globalization and its global governance structures are often interpreted as products of its technical architecture. Two views are put forward. The first considers how the Internet *facilitates* global governance. Proponents of this view argue that the Internet has empowered new actors – from activists to bankers to organized crime and terrorist networks – and that the way these actors operate (outside of the jurisdiction of sovereign states) has ushered in a new kind of governance environment in which states compete with them for authority and legitimacy (Anheiner, Galsius, & Kaldor, 2001; Brachman, 2006; Deibert, 2000; Y. H. Ferguson & Mansbach, 2004; Lipschutz, 1992; Naughton, 2001; Rosenau & Singh, 2002). The second view assumes that because the Internet's technological structure escapes territorial boundaries, and because its data flows can easily bypass the reach of conventional (i.e., national) political authorities, it is by *nature* an issue that demands global governance institutions and practices (Barlow, 1996; Kummer, 2005; MacLean, 2004; Mathiason, 2008). With the Internet's capacity for global governance articulated primarily as a matter of its empirical transcendence of states' territorial borders,

the technological determinism in both of these perspectives reflects the more general shortcoming of existing approaches to globalization and global governance: little to no attention is given to how globalization's ability to transform political order must contend with the state's political legitimacy, which is a product of discourses that inscribe sovereignty, not simply its territorial integrity.

This shortcoming is particularly problematic for the second perspective, given that the Internet began as a project of US national defence and was during its inception structured around logics of sovereignty and territoriality (Abbate, 1999). In light of the different definitions of the Internet described above, not only do the factors that allowed the Internet to be imagined and deployed in global rather than territorial ways need to be identified, but also how and why this 'global' scope and potential has been defined in different conceptions requires explanation. The neglect of contextual factors, in other words, provides a misleading account of the Internet's relationship with globalization and global governance.

Of course, it would be naïve not to recognize that the Internet's material properties push toward globalization (c.f. Galloway, 2004). But there is a complex interplay between the Internet's physical design and the normative context in which is evolves (c.f. Deibert, 1997b; McPherson, 2006). As Barney (2004, p. 41) states, "the destiny of the Internet is no destiny at all"; its eventual shape and form will depend not just on its material factors but their interaction with political conditions, values and interests (c.f. Bijker, Hughes, & Pinch, 1987; Misa, 2004).

Tracing the effect and consequences of metaphors as one element of the contextual factors that shape the Internet therefore attempts to explain both how it has become possible to assume that the Internet is a 'driver' of globalization and how this has generated specific

regulatory features. Attention to metaphors used to describe the Internet is not new (Anderson, 2005; Stefik, 1996). But no direct attention has been studied specifically to the way metaphors of globalization inscribe a specific normative meaning and what consequences they have for its governance. To investigate this, I draw from Lessig's (1999) thesis that the Internet is constituted by its modalities and principles of governance. A *global* Internet therefore requires principles and practices of *global* governance. But as argued, these principles and practices are first shaped and enabled by perspectives that become legitimated. Accordingly, the question is what perspectives influence (and in time determine) how "global" is defined in Internet governance. We can therefore still study the Internet as emblematic of globalization. But rather than focusing only on its physical diffusion across territorial borders, we can also examine how the Internet embodies the normative rearticulation and reconstitution of political order from territorially demarcated systems of governance to global ones.

Of course, metaphors are not the only thing that matters in uncovering how global Internet governance is shaped and structured. But that *global village*, *global marketplace* and *global war on terror* appear to correlate with developments in Internet governance begs the question of the effect these metaphors have had in influencing new priorities and policies for Internet regulation. Put simply, how do metaphors do the work they do? To reiterate, metaphors interact with and influence actors' perceptions and choices about what governance institutions and practices are 'appropriate'. My claim is not that they drive the construction of the Internet but that they, along with and at the same time as many other factors, contribute to this process by providing principles of political legitimacy through the establishment of political vocabularies and discursively defined practices that define and reproduce a given

view of political reality. The empirical work of this study therefore examines the circumstances which have made a given metaphor of globalization possible, how and why it becomes disseminated as a way to describe the Internet and in turn how these descriptions become inscribed as *the* way to conceive of the Internet through various institutionalized procedures. The IETF, ICANN and the evolving security roles for ISPs are therefore examined as products of the legitimating principles of global governance that become embedded as the popularity of the *global village*, *global marketplace* and *global war on terror* metaphors, respectively, exert specific influence on the broader discursive and material contexts that affect the management of Internet.

Although the metaphors are assessed chronologically, it should be stated that the ascendance of one metaphor does not necessarily abolish a previous metaphor. All of the metaphors – of globalization *and* of sovereignty – can be detected in any period. The objective of my analysis is to pinpoint the 'inscriptive moment' and delineate how the Internet's global governance was shaped in the context of these metaphors. But what this also does is shed light on the 'asymmetrical enrolment' of different globalization metaphors and their power relative to one another in different circumstances.

Implications for International Relations theory: wherefore the *sovereign* state?

International Relations theory's ongoing debates on the consequences of globalization for the sovereign states-system revolve around the relative power and prominence of the state vis-à-vis globalizing pressures (through financial, communication, and other transnational flows) and/or the purported distribution of political authority to non-state actors.

Proponents of globalization argue that the emergence of global governance institutions and practices is evidence that globalization transforms the topography of political life, and question the salience of sovereignty as a normative and conceptual lens for studying world politics. For them, to speak of 'inter-national' relations is a misnomer: as Scholte (2000, p. 49) argues, "internationality is embedded in territorial space; globality transcends that geography." It is therefore necessary to look beyond the field's 'state-centric' theoretical lenses to account for new structures of political authority and their contribution to the creation of a 'global' political order (Ruggie, 1993).

Critics of this position argue while global patterns and processes are unprecedented, politics ultimately rests within states and the states-system. They may, like Kissinger (2008), hold that globalization matters insofar as it changes the strategic objectives of the state so that globalization's impact rests in how it complicates the 'anarchical' relations between states rather than transforming the states-system (I. Clark, 1999). Or, they may agree that globalization has resulted in new kinds of 'global' governance institutions but consider them to be "[tools] of [state] power, not a substitute for it" (Pauly, 2002, p. 86) (c.f. Weiss, 1998). Others contend that while globalization may have disrupted state authority, the heightened security context ushered in after 9/11 signals a return to the state. In key issues such as security, the state has the legitimacy to act, suggesting that when it matters most, politics is about sovereignty (Acharya, 2007; Gray, 2002; Robert Jackson, 2007). The most radical theorists in this camp argue that globalization at most alters the conditions and requirements of sovereignty but does not dislodge sovereignty as the constitutive principle of political life; that is, globalization has resulted in a transformation of sovereignty rather than a transformation beyond it (Agnew, 2005; Brenner, 2004; Keck & Sikkink, 1998; Pauly &

Grande, 2005). The underlying assumption is that politics is by definition a matter of sovereignty, with states as the principal agents. Defining politics in this way does not prevent acknowledging globalization, but it does *a priori* rule out any possibility that globalization constitutes a transformation of political order.

As argued, proponents of the transformative thesis typically adopt an objective, empiricist stance of globalization, pointing to the cross-border movement of goods and services or the emergence of non-territorial forms of social actors and organizations as evidence that globalization has had detrimental consequences for sovereignty. Critics adopt a similar approach, pointing to the continued perseverance of the state, despite globalization, as evidence that politics fundamentally remains a question about state power. The neglect of discursive dimensions amongst globalization's proponents has already been discussed at length. But, failing to examine globalization discourses also results in shortcomings in the arguments of globalization's critics. Principally, the continued existence of the state is not on its own evidence of the continuing legitimacy of sovereignty. As discussed, sovereignty has discursive dimensions. Accordingly, it is necessary to consider the way discourses that support sovereign legitimacy, in the case of this examination, its constitutive metaphors, continue to hold force in ways that maintain the state as the epicentre of political power and authority. If, as will be elaborated in this study, this is no longer unequivocally the case, does this mean the end of the state? On the contrary, the reinscription of political order by globalization metaphors simply suggests that even if states persist, legitimacy might no longer be exclusively described through metaphors of sovereignty.

Maintaining the relevance of the state, without keeping the focus on sovereignty has several implications. First, it qualifies the study of globalization. As stated, global

governance institutions are relatively underdeveloped compared to the formalized bureaucracies of the sovereign state. Following the lead of Hall and Biersteker (2002a, p. 8), my investigation of post-sovereign forms of political authority does not claim that they are presently equivalent to or that they exceed the authority of sovereign states. Rather, I aim to address the instances in which the discourse and power of sovereignty are being fractured and is giving way to novel forms of global political legitimacy, power, and authority (c.f. Beck, 2005; Sassen, 2006).

Second, rather than assuming either that the state is compromised by globalization or that it remains unaffected by it, it opens up the field of exploring the possibility that states participate in globalization and global governance. This is not meant to suggest that globalization is entirely a state-driven process, thereby disqualifying claims about globalization's challenge to sovereignty (Weiss, 1998). But it demonstrates the ways in which the legitimating context of state action has moved away from sovereignty to more global political objectives such that state roles and identities have been redefined within emerging global structures of authority (Beck, 2005; Rosenau, 2003; Sassen, 2006). For this reason, criticisms that globalization lacks salience because of the continued existence of the state is not sufficient evidence of the continuing power of sovereignty – *de facto* or *de jure*. Although this investigation focuses on the emergence of putatively 'global' political structures, it does not ignore the role of the state.

In particular, the case explored in this study – global Internet governance – puts particular attention on the United States. In part, this is because of the Internet's development within US government agencies. However, it also speaks to broader dynamics of globalization. As many analysts have noted, the US has enjoyed a hegemonic role in laying

the groundwork of the principles that have shaped the contemporary global order. For this reason, globalization is often defined as US hegemony, or in the more extreme, as US Empire (Callinicos, 2005; N. Ferguson, 2004; Harvey, 2005a; Pieterse, 2004; N. Smith, 2005). But this can produce an oversimplified story of globalization that fails to consider how it has been applied with different effects, has been deployed and adopted with different objectives – at times as a resistance to US power – and has subsequently evolved as a complex phenomenon in which US power must contend with a number of different globalizing logics. Several commentators have noted that although the US has played an important role, "[a] time may be approaching … when … the institutionalization of globalization in various global forums might augur its continuation without domination by the US government" (Agnew, 2006b, p. 138) (c.f. Hardt & Negri, 2000; Hardt & Negri, 2004). Although it may be relatively uncontroversial to attribute a hegemonic role to the US in the genesis of the current global order, the tendency to reduce globalization to US power must be tempered by considering how its prominent role has generated complementary and competing globalizing processes.

Yet embedding the state within discourses of globalization should not discount the continuing salience of sovereignty and territoriality in some sectors or regions. Globalization to date is an uneven process concentrated in the 'global North.' Furthermore, globalization has not been an uncontested process. The ways globalization has challenged the state have often resulted in a retreat to national or even more local, tribal, and fundamentalist identities as a way to 'protect' against the influence of global governance (Agnew, 2006b; Castells, 2004; O'Brien, Goetz, Scholte, & Williams, 2000; Rosenau, 2003). But even these developments should not necessarily be dissociated from globalization. For some analysts,

the territorial conflicts in regions such as the Middle East cannot be fully explained by conventional logics of sovereignty but require understanding how they manifest within broader globally defined normative frameworks – such as, for example, an imperial globalization driven by the United States (N. Smith, 2005). Others examine the way that resistance to globalization is in fact a central dimension of the emerging logic of global politics. Anti-globalization, in their evaluation, is a misnomer (Amoore, 2005; Eschle & Maiguashca, 2005; Held & McGrew, 2002; Rosenau, 2003). Even if resorting to local/national identities undermines globalization, such resistance still highlights the emerging force – indeed, might themselves be an example – of globalizing power structures.

Methodology

This study explores the degree to which metaphors of globalization have contributed to the construction of global space as a political order, evidenced in the production of various global governance institutions and practices. The overarching objective is to explore whether globalization exists not only as a set of empirical, quantifiable flows but as discourses that shape understandings of political legitimacy. Examining globalization's discursive dimensions as a process of *metaphorical reinscription* and considering their consequences for global Internet governance, this inquiry is an empirical exercise that inquires into the conditions that allow for the suggestion of a metaphor and then traces how it participates in the production of political orders and their governance institutions and practices. It requires a specific methodology.

Broadly speaking, the political significance of metaphors has been studied in one of two ways. The first relies on a cognitive and subjective approach, with the focus on how individuals formulate, identify, and process metaphors as special linguistic constructions (M. Black, 1979, 1981; Charteris-Black, 2004; Davidson, 1978; Goatley, 1997; Kittay, 1987; Lakoff & Johnson, 1980; Musolff, 2004; Nogales, 1999; Semino & Culpeper, 2002). A second approach examines metaphors as cultural artefacts and examines how they contribute to developing intersubjective understandings within a given community (Beardsley, 1981; Bono, 2001; Booth, 1978; Edge, 1974; Goodman, 1981; Nietzsche, 1911; Richards, 1981; Ricoeur, 1977; Rorty, 1991; Searle, 1981). This second approach to metaphorical analysis uses an interpretivist methodology. Given the theoretical framework's emphasis on metaphor's discursive legitimation of political order, an interpretive methodology is better suited than a cognitive one.

This study uses the interpretivist tools of *genealogy* and *critical discourse analysis*. (Bartelson, 1995; Clifford, 2001; Devetak, 2001; Fairclough, 2001; Foucault, 1972, 1984; Hansen, 2006; Howarth, 1995; Laclau & Mouffe, 1985; Nietzsche, 1989). Genealogy identifies the historical conditions and 'micro process' which result in a metaphor's suggestion, the complex interaction and negotiations between different actors that persuade diverse groups to adopt the metaphor and its political vocabulary, and the material conditions and historical events that empower one metaphor, allowing its linguistic descriptions to prevail. It demonstrates how the intersection of events and processes naturalizes and normalizes a specific set of metaphorical descriptions as 'factual'. Furthermore, it explains the disruptions and ruptures of meaning that lead to the delegitimation of entrenched metaphors and the inscription of new ones.

This genealogical investigation is conducted using *critical discourse analysis* (Bartelson, 1995; Clifford, 2001; Devetak, 2001; Fairclough, 2001; Foucault, 1972, 1984; Hansen, 2006; Howarth, 1995; Laclau & Mouffe, 1985; Nietzsche, 1989). Critical discourse analysis allows the analyst to identify metaphors and their political vocabularies, determine the normative perspective embedded within them, consider how widely a metaphor is circulated, and connects practices to the metaphors that enable them, thereby linking the study of metaphors directly to their performances. Because metaphors and their vocabularies are circulated in everyday language, which is contained in multiple written and oral forms including speeches, reports, books, fiction, newspapers, constitutions etc.,[23] the methodological focus is placed on 'reading texts' (Hansen, 2006; Howarth, 1995).

Taken together, investigating *metaphorical reinscription* involves four methodological tasks:

First, as metaphors are triggered by and operate as part of a confluence of historical events, actors and material conditions, a discussion of the context in which a metaphor is suggested and how these influence its adoption is required. The objective of this step is descriptive. This examination allows me to reconstruct the 'environment' in which a new way to describe political order emerged and how different factors influenced the dissemination of a given metaphor, enabling it to create collective endorsement of certain vocabularies.

Second, a focus is placed on explicit articulations of the metaphor and its political vocabulary. Discourse analysis is not about hidden meanings or 'reading between the lines'.

[23] Texts need not be limited to written and oral forms. War monuments, films, art, music, and photography, amongst other things, can be treated as texts, as they project a certain vocabulary, set of social meanings and authorize certain kinds of practices. See Brassett (forthcoming), Weber (2002), Forum on 'Art and Politics', *Review of International Studies* Forthcoming)

If a particular metaphor creates and shapes reality, the 'world' is spoken about and expressed in particular words and statements. The primary objective is to locate the metaphor in scholarly, popular, news media, amongst others, and triangulate between them to determine the degree to which the metaphor saturates discussions of political order.

It is important to note that studying metaphors and their political vocabularies separately may be required as the metaphor is expressed through its political vocabulary and, as is often the case, literalized and fades from view. Delineating the metaphor's vocabulary also requires identifying the explicit articulations of the vocabulary across a variety of texts. Using the technique of 'linking', I establish which terms in a political vocabulary are 'linked' to a metaphor and to each other to create a coherent system of meaning.

Third, because discourse operates relationally, an intertextual approach is used to assess not only how certain terminologies and statements are connected as a political vocabulary, but also how this vocabulary differentiates itself from other concepts and how these distinctions are legitimated. This attends to the way a vocabulary is negotiated by different actors before they are put into circulation as 'facts'. Specifically, I try to determine how a particular metaphor of globalization and its vocabulary are juxtaposed against vocabularies of sovereignty and those of other metaphors of globalization.[24] Doing so reveals whether the legitimacy of the *state of nature* metaphor and sovereignty's normative nexus between *territory*, *population*, *authority* and *recognition* is put into crisis and replaced by a new 'description'. It also allows me to examine how different metaphors of globalization disrupt and displace each other.

[24] Hansen (2006, p. 44) explains that not all texts will explicitly juxtapose themselves against a contending political vocabulary. Often times, there is an assumed audience for the text that will understand the links and differentiations in play, especially after a metaphor has become commonplace. Differentiations in these instances can be implicitly deduced.

Finally, because metaphors are not simply about words, but words in 'play', the practices that are connected to and instantiate the metaphor must be made evident. This task entails two steps. First, it describes how an ascending political vocabulary translates actors' interests and identities so that they take on specific roles that fulfil the metaphor's political objectives. As these activities become consolidated, I evaluate this by examining how discussions of governance shift over time from a focus on the role of specific groups to more formal institutions of political authority. Second, I delineate the discursive space opened by formal institutional texts – such as operational guidelines, constitutions, etc. Doing this allows me to delineate which practices become prescribed as 'logical' and 'necessary' for the political order to function. I therefore am able to describe how the repetition of certain practices ratifies a given metaphor as the framework for legitimate governance.

The limits of space prevent detailed presentation of the full spectrum of texts in which a given vocabulary is manifest. I therefore provide a summary of my study of these texts, drawing out the principal ways in which the vocabulary was negotiated, settled upon and in time sedimented as 'fact'. Of course, a detailed content of particular texts and documents will be provided when especially crucial for illuminating of the specific modalities of *enrolment* or *transformation*.

Cumulatively, these four tasks develop a narrative that specifies the contribution of metaphors to the construction of political orders – that is, their legitimating role.

Case: Global Internet governance and the IETF, ICANN and ISPs

As described above, this exploration is grounded in a study of global Internet governance. Internet governance raises a puzzle for conventional assessments of globalization that put

emphasis on the ways in which the Internet's cables and routers stretch across the surface of the planet. Because the Internet was not born as a physically-global technology, the conclusion that it necessarily leads to globalization and radical shifts in politics fails to appreciate that the 'global' Internet was *constructed*, a product of a series of fierce debates and negotiations that gradually delegitimated its use as a defence technology and released it from the control of US defence agencies and their Cold War security objectives. In this way, the case of global Internet governance brings the question of the normative interpretation of 'deterritorialization' and globalization to the centre of debates about globalization and global governance. Although developments in Internet governance cannot be said to be a microcosm of the consequences of globalization in other areas, it is illustrative of globalization's discursive dimensions.

My study is divided into three different periods, each identified by the explicit articulation of a particular metaphor of globalization and the prevalence of a specific set of governance institutions and practices:

1. the *global village*'s emphasis on 'open access' and the creation of the *Internet Engineering Task Force* (IETF) during the late 1980s and early 1990s
2. the *global marketplace*'s commitment to 'competition' and the formation of the *Internet Corporation of Assigned Names and Numbers* (ICANN) during the mid-to-late 1990s
3. the *global war on terror*'s ratification of 'global security' and the reinvention of *Internet Service Providers* (ISPs) amidst growing concerns about terrorist use of the Internet.

The objective is not to justify or establish the prominence of these organizations. Histories of the Internet and its governance by historians of science and technology, political economists and practitioners have described these as three of the most prominent Internet governance

institutions (Deibert, Palfrey, Rohonzinski, & Zittrain, 2008; Geist, 2008; Hafner & Lyon, 1996; Hofmann, 2005; McTaggart, 2004; Mueller, 2002; A. L. Russell, 2006). Moreover, the analysis of Internet governance is sometimes periodized, with governance evaluated as the change from the prominence of IETF to ICANN and now the evolving roles of ISPs. These cases therefore can be used as signposts for the way global Internet governance more broadly speaking has changed over time. These organizations have not controlled the Internet – such a task is not only impossible given its decentralized structure but also because the actors and issues involved in the global Internet governance is too tremendous to be fully accounted for. The IETF, ICANN and ISPs can be considered 'snapshots' of the key issues and patterns of governance in a given time.

Although many of these assessments tend to consider the governance debates 'global' because of the Internet's technical features, they do not fully neglect the context in which these debates occur. However, in many instances context is treated more as what is happening in 'background' rather than integral to the process by which understandings of the technology and its governance priorities changed. When context is given due attention, as in Mueller's (2002) seminal study of ICANN, it is studied for the way it triggers actors pursuit of rational self-interest amidst changing economic conditions. While this is important, particularly in explaining the development of *networks of action*, what is assumed is that actors understanding of and interests regarding the Internet remain the same. What attention to discursive factors – in this case, metaphors of globalization – reveals is how the terms of debate are shaped by particular vocabularies and that the adoption and deployment of certain metaphorically defined terminologies by different actors actually shapes their interests and objectives, their ideas about what is considered legitimate to do in Internet governance and,

as a result, what instruments and policies are appropriate for achieving or maintaining those goals. Simply put, attention to the prevailing metaphors in each of these periods contextualizes events, actors and technical developments within shifting debates about what it means for the Internet to be 'global' and how these different understandings of 'global' over time and in different contexts resulted in different governance priorities, institutions and practices. My investigation of these cases therefore considers the specific and unique effects that metaphors had in affecting these debates and developments in global Internet governance.

Situating global Internet governance within a more general study of globalization's discursive dimensions requires not only showing that the global governance of the Internet has changed, but that such changes have also delegitimated sovereignty. This claim has been widely contested. One set of scholars agrees that the Internet has been defined and governed in different ways as a 'global' technology. But they argue that unlike other global issues, such as finance and the environment, the Internet has from the outset developed in the hands of civil society and private sector actors rather than governments (Drake, 2004, pp. 123-124; Hofmann, 2005; Kummer, 2005; MacLean, 2004). Because of this particular history, these critics contend that global Internet governance cannot illuminate the disruption of sovereignty. This view, however, fails to account for how the Internet developed under the auspices of state control as a technology of *sovereign* national defence, and that in some circumstances, as this study will demonstrate, the globalization of the Internet has been the result of states relinquishing their sovereign control. The global governance of the Internet is therefore a 'fact' to be explained, rather than assumed. Another school of thought argues that states have shaped Internet governance (Drezner, 2004; Mueller, 2002). Even if it is 'global',

it is product of sovereign interest. For some, global Internet governance is nothing more than the replication of *international* regimes (Mathiason, 2007, 2008; Mueller, 2002). This line of argument, however, tends to conflate the presence of states as evidence of sovereignty. When sovereignty is assessed discursively, state activity is not sufficient evidence of the continuing power of sovereignty. The discursive context in which states participate must be examined. I will try to show that although states remain relevant, the discursive context of global Internet governance has shifted away from sovereignty.

It is important to note that governance challenges for the Internet also manifest at local (e.g., programs for implementing the Internet in a school system), national (e.g., policies ensuring that the Internet be made available to all citizens), and regional (for instance, the European Union's 'Information Society' initiative) levels. Acknowledging this is important because the Internet has been associated with many different metaphors – for instance, the Clinton Administration's 'Information Superhighway' Initiative. While a particular metaphor may influence the Internet's global governance, a different (perhaps even contradictory) set may be employed in local, national, and regional contexts. Global Internet governance is therefore not examined as a matter of the planetary flow of Internet communications (which is a factor for all levels) but as a study of the circumstances in which the 'global' is invoked as a normative space to manage the Internet.

Sources

Consulting a wide variety of sources can better represent the diversity of opinions and interests involved in the negotiations and contestations that have installed certain metaphors and their vocabularies as the legitimate frameworks for global Internet governance. Although

my focus is on primary documents, secondary sources are consulted when they provide greater insight into how a particular metaphor or political vocabulary came to be prominent or provide relevant information about the people, processes, and events involved in the constitution of global Internet governance in a particular period. When secondary sources are frequently cited by the actors under study or historians commenting on the period they are treated as primary texts.

My sources are organized into six clusters. The general discussion of each globalization metaphor and its relation to the Internet examines scholarly texts, newspapers articles and editorials, popular books, and, where relevant, policy documents by governments, international organizations, or private actors. These are used to provide the context rather than study the precise mechanisms of enrolment. To study inscription more directly, I first consult 'histories' of the Internet which are often biographies not only of the Internet but also of the key actors and events that resulted in shifting contexts and priorities. Included in these documents are archived and published interviews with individuals involved in developing the Internet and/or its global governance institutions. Recognizing that technical questions are central to Internet governance, analysis is also focused on standards documents, where relevant (for instance, IETF's *Request for Comments*). The focus of these documents is not exclusively on the purely technical dimensions of the Internet but also the context in which these features should be applied. In this way they provide a useful metric for assessing how the priorities and frameworks for managing the Internet have changed.

Because governments are involved in this debate, I consult policy documents from governments and regional and international organizations. Given the history of the Internet's development, the majority of these documents are from US government agencies, including

the Department of Defense, the Advanced Research Projects Agency, the National Science Foundation, and the Department of Commerce. As civil society actors, corporations, business and users have taken active roles in the governance of the Internet, statements and publications regarding their views of Internet governance are reviewed. Examining the inscriptive work of non-linguistic behaviours requires evaluating documents that outline their operational procedures, codes of conduct, bylaws, and other documents, such as legal statutes and bills, etc. which delineate specific functions for the IETF, ICANN, and ISPs.

This study focuses on 'English' language metaphors. The Internet is has achieved more advanced penetration in the Western countries, which have been at the forefront of Internet governance discussions. But my analysis has examined documents from sites in which participants from different regions have been involved. Why English has been the preferred correspondence language certainly has much to say about the relative power dynamics in world politics more generally speaking, a question outside the scope of this analysis.

Organization

The three metaphors under study – *global village*, *global marketplace*, and *global war on terror* – translate into three empirical chapters, one for each metaphor. In the concluding chapter, I summarize my argument and findings and reflect upon their theoretical and practical implications for the study of globalization, global governance and the Internet within International Relations scholarship. I also consider possible avenues for future research.

Chapter 1

Global Village: 'Open Access' and the Internet Engineering Task Force (IETF)

The new electronic interdependence recreates the world in the image of a global village.
~ Marshall McLuhan, *The Gutenberg Galaxy*

ARPA's network, designed to assure control of a ravaged society after a nuclear holocaust, has been superceded by its mutant child the Internet, which is thoroughly out of control, and spreading exponentially through the post-Cold War electronic global village.
~ Bruce Sterline
(*Magazine of Fantasy and Science Fiction*, Feb 1993 <http://w2.eff.org/Net_Culture/internet_sterling.history.txt> accessed 8March 2008)

Introduction

Rorty argues that because a metaphor is 'absurd' according to conventional linguistic practices, it is "a use of language as yet insufficiently integrated into the language game to be captured in a dictionary entry" (Rorty qtd. in Calder, 2003). A first step in evaluating a whether a metaphor has contributed to the construction of a political order is to examine whether it can be found in a dictionary, a community's definition of 'facts' and 'reality'. In the context of global Internet governance, one would look for how the Internet's political potential is defined with respect to a metaphor of globalization.

The *Oxford American Dictionary* defines the *global village* as "the world considered a single community linked by telecommunications." *Encarta* defines it as "the whole world considered a single community served by electronic media and information technology." Wikipedia makes the connection between the Internet and the *global village* metaphor most

explicit: "Today the global village is mostly used as a metaphor to describe the Internet. The Internet globalizes communication by allowing users from around the world to connect with each other. … This new reality has the implication for forming new sociological structures within the context of culture." In all these definitions, the Internet is seen to provide the infrastructure for shaping the "whole world" into a "single community." As the Wikipedia reference puts it, the *global village* is the sociological and cultural structure inherent in the Internet. Although subsequent chapters will demonstrate that the Internet has been 'defined' using different global metaphors, the continued importance of the Internet in definitions of the *global village* demonstrates how the conceptualization of one has become intertwined with the other.

This chapter explores the history behind the linkage of the Internet to the *global village*. By showing the influence of the metaphor in shaping vocabularies, perceptions and practices of Internet governance, it provides a counter-point to accounts that assume that the *global village* is an intrinsic feature of the Internet's technical architecture – i.e. its decentralized planetary reach. Although, as argued in the Introduction, there is an element of technological determinism in the majority of opinion regarding the Internet's connection to contemporary globalization, due to the popularity of cyberlibertarian theories about the radical potential of cyberspace, the tendency is most pronounced when the Internet is discussed within context of the "global village". Considering the influence of the *global village* as a metaphor that became *inscribed* into the Internet imaginary, rather than inherent in its technical code, is important for two reasons. First, the idea of a *global village* predates the Internet. It has its roots in the post-war period's aspiration for building a more peaceful, harmonious world society. The assumed connection between the Internet and the realization

of this new kind of world order was a result of the popularity of Marshall McLuhan's cybernetic theories. Although articulating his cybernetic worldview well before the popularization of the Internet, McLuhan's focus on electronic communications was considered a prescient forebear, almost a prediction. Thus, the view that the Internet was a global village was established well before it 'arrived'. Second, as stated, despite the Internet's assumed 'global' status, it was initially developed for national defence purposes. Because it could be both a technology of *national* security and the *global village*, the Internet's eventual definition as a *global village* requires attention to the changing political environments in which the technology was adopted and deployed. Taking note of the above circumstances, of course, does not dispute that the technological developments that made it possible for the Internet to actually extend across the planet were necessary for the Internet's to become a 'global' technology. However, that this globality was interpreted as enabling a "global village", I contend, must explore the actions taken to articulate the Internet's technological capacities within a particular discourse of globalization.

Although the *global village* continues to be a popular metaphor for the Internet, in this chapter I focus on the 'initial' encounter, which also marks the beginning of the Internet's transformation from a 'sovereign' to a 'global' technology.[25] Again, the argument presented here should not be taken to imply that the metaphor alone is responsible for changes in Internet governance. A metaphor's 'stickiness' relies on its convergence and interaction with a number of different developments that reinforce its normative perspective. In this specific instance, I examine how the *global village* operated as a backdrop of

[25] I say 'beginnings' because subsequent chapters will show that even when the Internet was constructed as a global village, issues of sovereignty in other dimensions remained. Subsequent metaphors of globalization not only show how the discursive force of globalization has been redefined but also how different aspects of sovereignty have been challenged.

computing research. Operating as a backdrop means that there is little explicit reference to the metaphor during this period. Still, the metaphor was consequential. Primarily, its influence can be discerned as the academic preference for 'open access' principles converged with the *global village* metaphor's political tenor. This produced a new vocabulary for describing the Internet. The adoption of this vocabulary by both academics and governments (specifically the United States through the actions of the National Science Foundation), and in time the emerging community of Internet users, undermined use of the Internet exclusively for national security purposes. In time, the sovereign security apparatus that had created the Internet dissipated, giving way demands that it be constructed as a global, public, communications medium.

These developments culminated in the creation of the *Internet Engineering Task Force* (IETF), the Internet's pre-eminent standards-making body and considered to be the epicentre of the Internet's global governance in the early to mid-1990s (Barsook, 1995; Hofmann, 2005; Mueller, 2002; A. L. Russell, 2006). Because of its open, grassroots, participatory approach to developing the Internet's technical standards, the IETF was considered emblematic of the how the Internet could foster a *global village*. As commentators of the period note, "When the post-territorial visionaries looked for a model of Internet governance, [the IETF was] their main inspiration" (Goldsmith & Wu, 2006, p. 25).

Globalization, the *global village* and the Internet

The *global village* metaphor harkens back to the political movements of the 1960s, which invoked it as an alternative to the antagonistic politics of the Cold War. Predating the Internet, the metaphor related more to the ways in which the environment, human rights, economic flows, and the threat of nuclear destruction generated planetary webs of human interdependence. This sense of planetary oneness was reinforced when NASA released its 'whole earth' images. Viewing the planet as it appeared in outer space seemed to belie the gritty Cold-War conflicts that typified political life on the ground. As one commentator put it, "to see the earth as it truly is, small and blue and beautiful in that eternal silence where it floats, is to see ourselves as riders on earth together, brothers on that bright loveliness" (MacLeish, 1968) (c.f. Cosgrove, 2001, pp. 235-268). Advocates of the *global village* therefore argued for the reorganization of world politics in ways that encouraged and implemented greater global communication, collaboration, and cooperation (Fuller, 1970; King, 1970; Lovelock, 1987; Ward, 1966) (c.f. Cosgrove, 2001, pp. 235-268).

Advocacy of the *global village* as a political alternative gained momentum in the late 1980s and early 1990s. Like its initial articulation in the 1960s, the metaphor was underwritten by cosmopolitan visions of world community, which challenged not only the efficacy of the sovereign state to provide security but also its desirability. After the experience of two world wars and in light of the violent nationalisms that followed the end of the Cold War, sovereignty was considered to create misplaced and hostile distinctions by grouping an otherwise united humanity into (national)citizen-friends and foreigner-foes (Bohman & Lutz-Bachmann, 1997; Held, 1995; Linklater, 1998) (c.f. Walker, 1993). Its concern for security was thus a self-fulfilling prophecy of the threat of war: by defining the international system in terms of a *state of nature* marked by perpetual security dilemmas,

relations between states were destined to be hostile because opportunities for peace were precluded by (metaphorical) definition. As an alternative, cosmopolitans promoted a society based on humanity's rights and responsibilities. Championing human rights and devising new kinds of global democratic governance were thus the focus of scholarly, popular, and policy discussions when the end of the Cold War generated discussions about the possibility of a 'new world order' (Archibugi, Held, & Koehler, 1998; Commission on Global Governance, 1995; Held, 1995; Linklater, 1998; McGrew, 1997). The *global village* as a philosophy was evident in the title of one prominent scholar's reflection on the need for political change: creating "Alternative Visions" to sovereign politics was about finding "Paths in the Global Village" (Dallmayr 1998). In short, the *global village* sought to globalize political community and authority with a vocabulary of deterritorialization – removing the mutually exclusive notion of *territory* as the basis of political community, *population* was redefined as humanity, *recognition* as respect for individual rights and freedoms, and *authority* as a system of global-cosmopolitan, not sovereign, governance.[26]

Descriptions of the Internet as a *global village* usually reference the work of Marshall McLuhan (1962; , 1994). His conclusions that electronic communication was a globally integrated central nervous system producing kinship relations on a planetary scale continue to be considered as a prescient and apt description of the Internet.[27] Although McLuhan popularized the term well before the Internet was invented, one commentator notes that because "[he] made the idea of an integrated planetary nervous system a part of our popular

[26] Whether cosmopolitanism could actually achieve this or whether it was a guise for a different kind of political power has been widely debated. For prescient criticisms of liberal-cosmopolitan theory see (Brennan, 1997; Cheah & Robbins, 1998; Cosgrove, 2001; Hardt & Negri, 2000; Shah, 2006; Walker, 2003).

[27] Reference to *the global village* can also be found in Wyndham Lewis's (1949) *America and Cosmic Man*. Buckminster Fuller also laid claim to the idea. Fuller praised McLuhan's genius for the way he interpreted the *global village* and popularized it.

culture … when [the Internet] arrived in the global village, it seemed no less amazing, but still somehow part of the natural order of things."[28]

The Internet's ability to facilitate communication across traditional territorial boundaries was immediately considered the literal expression of the *global village*— if not immediately so, at least it could develop the communications and relationships needed so world politics could be transformed into a more peaceful form. Dodge and Kitchen (1998, 4) argue that by the time of the Internet's popularization in the late 1980s and early 1990s, the view that it would "transcend the differences between cultures and societies to create a new *global village* where people will come together and work towards mutual trust and understanding, [and] create a world that is 'smaller' and more 'democratic'" was firmly entrenched in the popular psyche (c.f. Turner, 2006).

The most vocal proponents of the Internet's 'global' transformative potential invoked cyberlibertarianism, which was articulated in political credos by media celebrities such as Nicholas Negroponte (1995) and John Perry Barlow (1996) and, under their direction, in the pages of *Wired* Magazine (Flichy, 2007, pp. 155-179). In this perspective, because Internet cables, networks, and servers evade conventional territorial jurisdictions, the Internet's technical architecture makes it impervious to governmental control and thus libertarian by nature. As a result, cyberlibertarians promoted cyberspace as a "new social space, global and anti-sovereign, within which anybody, anywhere can express to the rest of humanity whatever he or she believes without fear" (Barlow, 1996). Cyberspace could become a "new

[28] ("Marshall McLuhan Foresees The Global Village") Available: www.livinginternet.com/i/ii_Mcluhan.htm [Accessed 6 June 2007]. McLuhan cautioned that globally integrated electronic communications could produce a more peaceful and harmonious world community just much as they could foster totalitarianism and terror. The conception of the *global village* associated with the Internet usually refers to its more optimistic potentials.

frontier, where people live in peace and free from government meddling" (Barlow, 1996) (c.f. Godwin, 2003).

Whereas cyberlibertarians sought to escape the repressive power of sovereignty, as expressed in the coercive legal and military authority of governments, by moving to the 'virtual communities' of cyberspace, others saw the Internet as the means by which to transform the 'real' world of sovereign states. For example, attention to the Zapatista struggle and the success of the anti-MAI campaign drew attention to the role of the Internet in organizing and mounting effective political protests against governmental policies at home and abroad (Deibert, 2000; N. Klein, 2002; Stephen J Kobrin, 1998; Naughton, 2001). Especially for those participating in political campaigns with a transnational scope, Internet use to communicate and collaborate gave birth to a new '*global* civil society' (Anheiner, Galsius, & Kaldor, 2001; Deibert, 1997b: 163; Lipschutz, 1992).

Alongside these views, albeit with less visibility, others promoted the Internet's ability to promote greater freedom and communication because it was, at least at the outset, outside the reach and control of the corporate media conglomerates. The Internet was 'free' not only because it evaded governmental control but also because no one owned it so the information that flowed through its interconnected networks was freely available. Because users were both consumers *and* producers of content, instead of the traditional media model of one-to-many communication, the Internet promoted a new logic of many-to-many communications. This non-proprietary, many-to-many model of open dialogue reinforced the idea that the Internet facilitated a global democratic agora (Mosco, 2004, pp. 30-31; Mueller, 2002, p. 56; Wolin, 1993).

These discourses represent different and even divergent political philosophies. Whereas cyberlibertarians prized the Internet because of its capacity to enhance individual freedoms by providing an escape from the reach of governments, global civil society advocates were inspired by the way it shifted the political focus to individuals in order to generate a greater sense of responsibilities and obligation to humanity as a whole. Both of these views stood in contrast to the commons approach, which put forward a collectivist vision of global society. Cyberlibertarians, for instance, would be vocal proponents of the future commercialization of the Internet and its development as a platform for electronic commerce (Flichy, 2007, pp. 155-179; Valovic, 2000, pp. 155-160). However, taken together these perspectives created the expectation that the Internet – in real or cyberspace — held the potential to "[annihilate] social divisions that historically separated the world's people" (Mosco, 2004, p. 87). By allowing cross-border communications and cross-cultural dialogue, the Internet could overcome the distinctions and inequalities promoted by territorial identities – the simultaneity and instantaneity of its communications fostered a sense of individuals as members of a common humanity (Cairncross, 1997; M. Hauben & Hauben, 1997; Negroponte, 1995; Pemberton, 2001, p. 170).

This had a completely subversive effect on the system of states. As one commentator put it, "While politicians struggle with the baggage of history, a new generation is emerging from the digital landscape free of many of the old prejudices. These kids are released from the limitation of geographic proximity as the sole basis of friendship, collaboration, play and neighborhood" (Negroponte 1995: 230). Collectively, the Internet became the signature technology, and perhaps even the definitive feature, of a united global village polity (Deibert, 2000; Naughton, 2001). As Turner (2006, p. 1) summarizes, once "ubiquitous networked

computing had arrived … scholars, pundits and investors alike saw the image of an ideal society: decentralized, egalitarian, harmonious and free."

In time this understanding of the Internet gave birth to a new kind of political activism, specifically geared toward protecting the Internet from government surveillance and censorship and corporate control. With more recent commercialization of the Internet and governments' enhanced legal and technical capacities to monitor and filter Internet content, vociferous campaigns for open source software and freedom of expression and speech on the Internet today are evidence of the powerful hold the vision of the Internet as a *global village* continues to have for some groups (c.f. Deibert, Palfrey, Rohonzinski, & Zittrain, 2008).[29]

The popularity of the *global village* metaphor in discussions about the Internet is not without its critics. Different critics pointed to how vast sections of humanity, particularly in the developing world, lack the infrastructure for telephones let alone the Internet; how users were predominantly white, middle-class males (J. Katz, 1997; Wellman & Haythornthwaite, 2002); that governments were actively censoring material (Goldsmith & Wu, 2006; Lessig, 1999); that networks were often used more for local communication rather than fostering relationships between distant communities (Wellman & Haythornthwaite, 2002); that networks in fact imposed their own forms of political power and control (Barney, 2000, pp. 222-231; Galloway, 2004); that cyberlibertarian notions of 'community' were thin (Winner, 1997); and that Internet development promoted Western-centric, rather than culturally diverse, value systems (Ess, 1998). Celebrations of the emancipatory and inclusive nature of the Internet were deemed to be nothing but rhetorical hype, engaging in fantasies of the

[29] See, for instance, the work of the following groups: the OpenNet Initiative (http://opennet.net), the Association for Progressive Communications (http://www.apc.org), the Electronic Privacy Information Center (http://www.epic.org), and the Electronic Freedom Foundations (http://www.eff.org)

'digital sublime,' with little connection to the problems of networked communication (Mosco 2004). However, global villagers have far from neglected these shortcomings – they have become more attuned to the need to facilitate access for marginalized groups, a central focus of the United Nations' 2003 and 2005 *World Summit on the Information Society* (WSIS).[30] Thus for all its imperfections, the *global village* continues to be a political project and ideal that is accompanied by concerted political action.

What these criticisms have made apparent, however, is the technological determinism inherent in early discussions of the Internet (Lessig, 1999; Turner, 2006; Winner, 1997). If, however, the Internet's political potential involves its material factors intertwined with its governance frameworks, understanding its emergence as a central feature of the *global village* requires delineating the processes by which this metaphor became inscribed within the framework for global Internet governance. As stated, the Internet was initially developed to bolster US national security; it was therefore designed and developed according to the security impulses of the *state of nature* metaphor and the priority they placed on sovereignty.

These securitized 'origins' are a far cry from the decentralized, bottom-up, and deliberative politics that became associated with the Internet in the early 1990s. Because the IETF was lauded during this time as the perfect example of how the Internet could foster more global, deliberative politics, tracing its emergence sheds light the circumstances that put *global village* metaphor at the forefront of Internet debates and how and why this contributed to a shift away from the hierarchical and closed 'security' cultures that created the Internet to its development as a medium for anti-sovereign, 'global' politics.

[30] For instance, the WSIS *Geneva Declaration of Principles* stated: "We are also fully aware that the benefits of the information technology revolution are today unevenly distributed between the developed and developing countries and within societies. We are fully committed to turning this digital divide into a digital opportunity for all, particularly for those who risk being left behind and being further marginalized" (United Nations, 2003).

The sovereign Internet: survivability and 'restricted access'

Without the explicit normative impulses of the *global village* metaphor, how did the vocabulary of 'openness,' 'communications,' 'user-empowerment,' and 'grassroots deliberation' emerge as an alternative to the legitimating norms and practices of sovereignty? How, in other words, did the Internet evolve from its governance by the *state of nature* metaphor to that of the *global village*? In this section, I describe the 'facts' of Internet governance that were produced by the literalization of the *state of nature* metaphor and the legitimating power of sovereignty. I do not provide a full account of the enrolment into specific political vocabularies and networks of action. The purpose of this discussion is to lay the groundwork for understanding the disruptive significance of the *global village* metaphor and the enrolment strategies it triggered to produce a particular 'global' structure to Internet governance.

The single network project – the ARPANET – funded by the US Department of Defense and its Cold War national security imperatives does not put the history of networking technology exclusively in the United States, because other national networks were under construction, especially in Europe.[31] However, decisions and circumstances within the US played a significant role laying the groundwork for inter-networking (Internet) initiatives. The considerable institutional and monetary support provided by US government agencies also situated key events in Internet development in the United States (Deibert,

[31] In particular, Donald Davies, working for the National Physics Laboratory in the UK, without knowledge of research being conducted in the US, was investigating the requirements for networked communication. The two efforts converged after Davies heard Paul Baran, a researcher at the RAND Institute, deliver a paper on networking (J. O'Neill, 1990).

1997b; Dodge & Kitchin, 1998). The *state of nature* metaphor therefore has particularly prominent implications in US networking initiatives.

Historical accounts of the motivations behind the Internet's, or more specifically the ARPANET, development vary. According to one school of thought, the network was developed with the explicit goal of 'surviving' an imminent nuclear attack from the Soviet Union. Fears of losing robust and reliable communications in the event of a successful strike initiated research into survival communications systems (Abbate, 1999; Misa, 2004; Saco, 1999). This initiative is linked to the work of Paul Baran at the RAND Corporation, who explicitly researched decentralized and network communications with the objective of developing a communications system that could withstand enemy attack (J. O'Neill, 1990; Saco, 1999, p. 266). Other histories focus on the civilian origins of the Internet. In this second school of thought, the ARPANET project is seen as the innovative creation of the civilian subculture of computer science researchers interested in creating a time-sharing system that facilitated the exchange of resources on distantly located mainframe computers. This account emphatically denies any connections to military and defence objectives. Instead, Hafner and Lyon (1998, p. 10), its key proponents, argue that "the project had embodied the most peaceful intentions … [and] had nothing to with supporting or surviving war."

While it is an overstatement to say that this initial experiment in networking was exclusively developed as a tool of national defence, it is equally misleading to suggest that it was unconnected to military initiatives and objectives. Although the goal of overcoming an imminent Soviet attack may not have been the sole purpose behind the Internet's creation, the Cold War context in which ARPA and its mission were created matters (Flichy, 2007;

Turner, 2006). A cursory survey of the prevailing theories and accounts of world politics at the time makes clear that the *state of nature* metaphor defined and directed political objectives and strategies during the Cold War (Morgenthau, 1948; Waltz, 1959, 1979). This is not surprising given the experience of two world wars and the antagonism between Western countries and the Soviet Union. Even if peaceful intentions motivated the computer scientists involved in the project, defence objectives came to have greater importance and the final say (Abbate, 1999, p. 77; Misa, 2004, p. 249). Given the degree to which the *state of nature* metaphor at this point had been inscribed as the image of world politics, explicit references to the metaphor in the development of Internet governance are rare. Instead, evidence of that metaphor's influence is apparent in the political vocabulary of 'survivability' and 'restricted access' employed by key agencies involved in the Internet's development.

Somewhat defeated by the Soviet's success at putting the first satellite in space and the moon landing of Luna 2, the US government established the Advanced Research Projects Agency (ARPA) within the Department of Defense to try to overtake Soviet research and technological development. The national security mandate of the agency was made even more explicit in 1972 when ARPA was renamed the *Defense* Advanced Research Projects Agency (*D*ARPA) (R. Hauben, 2008; Herzfeld, 2008; Saco, 1999, p. 199). The ARPANET initiative emerged in this context. Even if initially considered a time-sharing system between large mainframe computers, the defensive importance of the ARPANET project was always lurking in the background (Abbate, 1999).

Emphasis on the security mandate should not diminish the fact that the ARPANET was an exciting experiment in computer science. However, it does provide the legitimating context of computing and networking research at the time. It was the Department of Defense,

through ARPA, that provided the source of funding and defined the applications of research. Consequently, although ARPA was mandated to fund basic scientific and technological research, the research itself was intended for military application and thereby tied to national security objectives. Despite what it became, the initial network was a product of defence objectives. As Abbate (1999, p. 144) explains, although the popular success of the Internet has allowed its military roots to be downplayed, the simple and adaptable network protocols that have become embedded in the Internet were "derived in part by the military's concern with survivability." An *impending* Soviet attack may not have been the explicit motivation for networking research but the need for robust defensive and strategic communications was a major US military goal and a major factor behind the research that eventually lead to the Internet's creation.

Concerns about security and survivability precipitated into *restricting* access to the network and the priority of defence over civilian concerns. In the first instance, use of the network was limited to defence officials. Civilians who were granted access consisted of only a small group of computer scientists contracted by ARPA to undertake the required research to design and build a workable network. In this sense, they were employees of the Department of Defense and were subject to its aspirations for the network. As one computer scientist involved at the time recalls, "Every time I wrote a proposal, I had to show the relevance to the military's applications" (Cerf qtd. by Abbate, 1999, p. 77). While Cold War fears were sometimes used to justify the funding of projects that people wanted to undertake anyway (Randall, 1997), ARPA itself was mandated under the Department of Defense and the ARPANET was justified to the Pentagon in military terms (Misa, 2004, p. 249).

That said, security concerns are strangely absent in much of the documented research activity that created the network. This is in part because principal investigators at the universities contracted by ARPA buffered the graduate students they supervised to build the ARPANET from the Department of Defense's agenda (Misa, 2004, p. 249). Graduate students may have worked in an environment that was either oblivious or dismissive of the network's defence and security context, but military imperatives drove their research. Of course it is possible that defence objectives were treated as mere platitudes, used only to justify research. If 'Washington' wasn't involved in the actual research, what effect could it really have? The answer lies in how the network was put to work rather than how it was made. Once the ARPANET was fully developed, the Department of Defense's authority over it increased. Because ARPA was mandated for research, completion of the ARPANET meant the researchers' mandate ended. By 1971, ARPA had to think about how it would divest its role in the network. As a defence agency responsible for conducting research for eventual military use, it could not transfer the network to an outside authority (academic or commercial) unless the military decided it had no use for it. But when in 1975 the Department of Defense decided it had a use, supervision and operational policy for the network was transferred to the Defense Communications Agency (DCA).

Further embedding the network in the organizational culture of national defence and security intensified restricted access requirements. This was a paradoxical development. A paradox first became evident in the DCA's desire to build a comprehensive defence communication system. Alongside the ARPANET, the Department of Defense and ARPA had successfully developed radio and satellite networks, which were also shifted to the DCA. Although the DCA wanted to retain the advantages of having specialized networks, it also

wanted universal communication among them (Dodge & Kitchin, 1998, p. 7; Mueller, 2002, p. 75). It therefore looked to ARPA to create an *inter-networking* protocol that would allow different networks to intercommunicate without losing their distinctive features and purposes.

ARPA researchers Vint Cerf and Robert Kahn responded with the Transmission Control/Internet Protocol (TCP/IP). This protocol allowed 'borders' between networks to be invisible. At the same time, it would allow different networks to be managed according to their own purposes and priorities. One the one hand, this protocol expanded access – different networks could access each other. However, as employed by the DCA, it was used only to further restrict access. Links could have been made between the ARPANET and networks that were developing abroad, but TCP/IP was made available to US defence networks only. Although inter-networking made possible not only the interconnection between the different networks used by the DCA as well as transnational connections, the security mandate of the DCA meant that only a few foreign networks – from allied countries – could interconnect to the ARPANET, and even then only under very strict regulations (Latham, 2005, pp. 167-168). Because the network was linked to national security, creating innumerable links to foreign networks increased the network's vulnerability to attack and therefore could potentially compromise the robust communications it was meant to ensure. Despite the deterritorialized image of today's Internet, the first 'inter-network' was rooted in concerns about sovereign security and thereby highly territorialized. The only borders that were made invisible were between networks located in the United States, and in rare cases its allies. The enemy-friend distinctions of the *state of nature* metaphor were embedded in the Internet's initial motivations and operational implementation.

The second dimension of the paradoxical desire to create universal communication while also restricting access developed when tensions grew between the use of the ARPANET by military personnel and the civilian defence researchers. Military personnel were concerned that civilian researchers did not always enforce the DCA's strict access controls. And, with new 'personal computers' hitting the market at relatively affordable prices, there were concerns about the network's vulnerability to attack, not only by foreign enemies but by hacker hobbyists (Abbate, 1999, p. 124) (c.f. Turner, 2006). Tensions emerged between the military objectives and the research ethos of the civilian researchers. While academic researchers prioritized 'open access' because it promoted the sharing of ideas, without strict access controls, it also meant that "somebody could … launch an attack" (BBN manager qtd. Abbate, 1999). In light of these growing tensions, in 1983 the DCA announced that it would separate military users from its contracted defence researchers. It created MILNET, for military users, and maintained the ARPANET for defence researchers. Because of TCP/IP, the two networks could intercommunicate but each would be managed according to its own needs and priorities.

In short, TCP/IP and the separated networks for military and civilian users had the potential to override restricted access controls. TCP/IP theoretically could allow networks in any part of the world to intercommunicate. However, access was restricted to US defence networks only, and in exceptional circumstances US allies. With the benefit of TCP/IP, the DCA created MILNET to further restrict access by excluding civilian researchers from the military's application of the ARPANET. Although this effectively made ARPANET a 'civilian network,' it still had restricted access because only those who were contracted by various defence agencies had permission to use the network.

Evidently, a specific set of 'facts' defined and structured the governance institutions and practices that created the Internet. With security and defence as the key governance objectives, the network's 'survivability' against attack was the 'why' behind the Internet's development and management. These objectives converged in TCP/IP and MILNET to define the 'what' of Internet governance as the management of networks tools of national defence. The effect of the *state of nature* metaphor was evident in restrictions on access. Restricted access described the 'who' of Internet governance as defence officials (or their contracted researchers). This in turn limited the 'where' of Internet governance first to ARPA and then to the DCA, both of which were under the Department of Defense. Such a hierarchical decision-making process, whereby directives about network design were issued from the Department of Defense and then operationalized by researchers, was 'how' the Internet was managed. Governance officials and governance sites were thus sovereign authorities, implementing their key concerns about national defence in the heightened security context of the Cold War. 'Restricted access' inscribed the *state of nature* metaphor into Internet governance through a vocabulary and set of programs around 'security,' 'survivability,' 'defence,' and 'attack.' Said differently, 'restricted access' was the performative logic of the *state of nature* metaphor, making visible the legitimating principle of sovereignty.

Legitimacy crisis: disrupting 'restricted access'

Although defence objectives and agencies set the context for the Internet's development, the actual work of developing technical standards fell into the hands of computer scientists.

Abbate (1999, p. 5) notes that from the outset, the governance of the Internet was marked by a tension between the Department of Defense's "command economy of military procurement, where specialized performance is everything" and the "research ethos of the university, where experimental interest and technical elegance take precedence over commercial application." Given ARPA's approach to delegating projects and leaving them to develop with minimal supervision from ARPA managers, the momentum shifted towards the research ethos of the project's university investigators. Because they operated with seeming independence, these scientists "incorporated their own values of collegiality, decentralization of authority and open exchange of information into the system" (Abbate, 1999, p. 5). In so doing, they set the conditions for a 'crisis' that undermined the legitimating security impulses that had first motivated the design and development of the Internet.

The shift of momentum towards the research community, and the subsequent disruption of 'restricted access' can be located in three interrelated developments. The first two emerged from within the management structure and technical protocols for the ARPANET implemented by the US defence agencies. The principal of these was the Network Working Group (NWG), which was formed by ARPA to promote dialogue among its contracted researchers about the technical requirements for the evolving ARPANET. Rather than attend the meetings themselves, ARPANET's Principal Investigators chose to send their graduate students. Left to discuss network specifications for a government-funded research project, the students were unclear about what authority they had. As one participant described it, "I had expected some formal action from Washington creating a project or designating someone in charge; I thought some pro would show up" (Crocker Interview in

Randall, 1997, p. 31). In the end, no one did show up and by default the development of the ARPANET was left in students' hands (Froomkin, 2003, p. 783).

Not only were the graduate students were embedded in an academic culture that stood at odds with the closed nature of military decision-making, many were also inspired and deeply affected by 1960s American counter-cultural movement (Turner, 2006). This exerted an indirect influence on networking culture in several ways. First, the counter-cultural movement had a distinctive tenor among university students on the US West Coast. This brand of 'west-coat libertarianism' repudiated military bureaucracy, closed and exclusive communities, and hierarchical decision-making processes. Because leading graduate students involved in the ARPANET were located at West Coast universities (such as Berkley, Stanford, University of Southern California), such values had a notable influence on them (Flichy, 2007; Hafner & Lyon, 1998; Poole, Schuyler, Senft, & Moschovitis, 1999; Turner, 2006). Second, this radical libertarianism influenced a new generation of computer hobbyists, resulting in the anarchical and anti-authoritarian principles associated with hacker culture. Although hacker culture developed in parallel with ARPA researchers (Flichy, 2007), many hackers had information-sharing relationships with Digital Equipment Corporation and Bolt, Baranek, and Neuman, the latter of which had been awarded the ARPA contract for the work required to develop and implement the ARPANET (Hafner & Lyon, 1998; Turner, 2006).

Third, Turner (2006) argues that the 'New Communalist' strand of the counter-cultural movement provided a philosophical ethos for computer and networking research. It is here that the *global village* metaphor begins to exert its influence over networking research. Although the New Communalists did not say anything about the ARPANET directly, its most famous member, Stewart Brand, interacted with Doug Englebart and Robert

Taylor, both of whom were involved in the development of the ARPANET. According to Turner (2006, p. 36), the New Communalists combined their ideas for a "new, less violent, and more psychologically authentic world" and its "rejection … of any and all formal chains of command" with an appreciation for technology, especially computers. In particular, they drew inspiration from McLuhan's (1962; , 1994) theory of the *global village*. Though McLuhan did not suggest his cybernetic *global village* would necessarily create a more peaceful human organization, Turner argues (2006, p. 54) that for the New Communalists "[the global village] did not need to refer to anything more dogmatic than the felt sense of generational togetherness". Reflecting on the broader political context of the time, Turner (2006) claims that "to a generation that had grown up in a world beset by massive armies and by the threat of nuclear holocaust, the cybernetic notion of the globe as a single, interlinked pattern of information was deeply comforting: in the invisible play of information, many thought they could see the possibility of global harmony." This (mis)appropriation of McLuhan has been called "McLuhanism without McLuhan" (Barbrook, 2008). Even though conventional histories of the Internet do not usually acknowledge its importance, Barbrook (2008) asserts that McLuhan's *global village* was "the dominant ideology of both radical and conservative intellectuals" involved in computing research.[32] Overall, the countercultural movement produced a set of radical computing principles that eventually were described through the utopian visions accorded to McLuhan's cybernetic theory of the *global village*.

The convergence of the countercultural movement with the graduate students involved in the ARPANET's development appears to have had a mutually reinforcing effect. Working within an academic culture, graduate students were accustomed to making decisions

[32] Few would deny McLuhan's iconic status in the 1960s. He was a prominent feature on the lecture circuit, with 'radical' students flocking to his lectures (Turner, 2006, pp. 41-68).

through practices of open dialogue and exchange of information. This deliberative model was also reflected in the counterculture movement's vision of a cybernetically enhanced *global village* world order, which favoured decentralized, anarchical community-based governance. Both prized 'open' rather than 'restricted' access to decision-making – academic or otherwise. To the degree that the ARPANET's graduate students were involved in and influenced by the countercultural movement, it seems reasonable to assume that the popular computing discourses disseminated through the *global village* metaphor lurked in the background of their deliberations about how to develop the ARPANET and what the objectives of networking should be (c.f. Barbrook, 2008; Turner, 2006). At minimum, then, it seems plausible to discern the influence of the *global village* metaphor on the period's networking research in the convergence between the academic and counterculture's preferences for 'open' access. It seems likely that had the ARPANET's management been put in different hands, for instance, if ARPANET had not been separated from MILNET and had been placed entirely under the authority of military and defence officials, its governance would have remained within the discursive context of the *state of nature* metaphor, or evolved in a different direction. Along these lines, one can assess the disruptive effect of the new metaphor on networking governance in the way '*open* access' challenged the 'restricted access' governance procedures and protocols associated with the Internet development under the *state of nature* metaphor.

The challenge to the defence hierarchy was not concerted or explicit, but gradual and subtle. Graduate students did not mount protests to the formal authority of defence agencies over the network. In fact, defence agencies themselves facilitated the influence of student academic and counter-cultural approaches to networking research. For ARPA, the NWG

provided an efficient way to manage the network. As Steve Crocker, a leading member of the NWG has reflected: “ARPA wasn’t stupid; it knew it had the best possible solution. Ideas were flowing, there was commitment from principal investigators, and there was a growing group of relatively inexpensive graduate students” (Crocker interview by Randall, 1997, p. 31). As a research agency, ARPA favoured delegating responsibilities to principal investigators and leaving them to develop with minimal direction. In fact, ARPA directors and project managers were often researchers themselves, with close connections to the universities contracted to undertake the new research. ARPA therefore supported the academic approach to research (Abbate, 1999; Hafner & Lyon, 1998). Even so, ARPA’s endorsement of the NWG created an opening for the development of governance principles and practices for networking management that were fundamentally different than those established by the broader security context.

The disruptive influence of this new ethos of computing and networking research was manifest in the NWG’s approach to making decisions about appropriate technical standards for the evolving ARPANET. Specifically, NWG students introduced four practices that collectively called into question ‘restricted access’ (and thereby sovereignty) as a legitimate principle for managing the network. First, not having formal authority over the ARPANET, the NWG felt that it could not impose formal restrictions on participation in its discussions. But more than this, they felt open discussion and debate would lead to better and more robust research outcomes. It also gelled with their resistance to making decisions through hierarchical institutional structures. Consequently, as Hafner and Lyon’s (1996, p. 144)(study of the period demonstrates, the NWG was designed as an “open club that all were invited to join.” Second, to facilitate this open debate, NWG discussions were documented in

a series called 'Requests for Comments' (RFCs). To promote a more creative and free-flowing discussion of ideas, RFCs eschewed the formality of academic publications by encouraging the publication of "philosophical positions without examples or other specifics, specific suggestions or implementation techniques without introductory or background explication and explicit questions without any attempted answers" (S. Crocker, 1969). In this way, RFCs were not just 'documents,' but active venues – agoras of a sort – where different ideas could be proposed and debated by anyone. RFCs therefore infused the NWG's network development with a deliberative ethic. Even though the NWG operated under a defence mandate, RFCs were not classified documents but made freely available. As Jake Feinler recalls, "This was no mean feat when you consider that [the NWG was] being funded by the [Department of Defense] during the height of the Cold War" (USC/ISI, 1999).

Third, the NWG made several technical design choices that required a specific approach to managing the network. Foremost among these was a commitment to open-architecture.[33] As Crocker recalls, "We were frankly too scared to imagine that we could define an all-inclusive set of protocols that would serve indefinitely. We envisioned a continual process of evolution and addition" (USC/ISI, 1999). As a result, users were given the power to propose new features. This 'user-empowerment' model provided a decentralized structure of network development. This decentralized management structure was augmented by the layered design of the network. Although primarily meant to reduce technical complexity in the system by organizing the network around discrete functions that different people were responsible for, these layers had to successfully interact with each other to be operational (Abbate, 1999, p. 39). 'Protocols' therefore had to have widespread support and

[33] Open architecture is a principle of computer design where users can see all parts of the Internet's architecture without proprietary constraints. It also enables them to add components and applications that are suited for their particular purposes.

were accordingly designed and accepted through a negotiated consensus (Hafner & Lyon, 1998, p. 145) A decentralized structure also imposed and implied an egalitarian approach to network design and decision making. Not only were different layers 'equal' but also, in order for the layers to interact, the consensus process required that different network participants had to be involved with equal status for a workable protocol to be designed.

Endorsed by ARPA, the NWG's approach to network design and development became the expected process for protocol development. But by supporting the NWG, the 'command and control' hierarchical system of network management inscribed by the security logics of the *state of nature* metaphor were, if not explicitly challenged and criticized by the students, unsettled and destabilized. That this occurred through the advocacy of 'open access' can be detected through the NWG's emphasis on an open, decentralized, grassroots (user-driven), egalitarian, and consensus-based approach for network management.

A second development that shifted the momentum to the computer scientists' 'open access' approach was a direct result of the TCP/IP's introduction. Although this protocol initially reinforced the 'security' ethos that initiated the development of ARPANET, even at the outset TCP/IP undermined 'restricted access.' ARPA researchers shared the DCA's desire for an internetworking protocol and therefore enthusiastically accepted the DCA's request that one be created, but it appears that this convergence of interests was not borne of common objectives. After a successful demonstration of the ARPANET at the International Conference on Computer Communications (ICCC) in 1972, ARPA researchers and their counterparts worldwide began to explore the possibility of connecting networks located in different parts of the world. Although Vint Cerf was an ARPA employee, he was also the founder of the *International* Network Working Group. Consequently his motivations in

helping Kahn design the internetworking protocol do not appear motivated by a desire to protect the US's territorial borders. Instead, he was interested in helping Kahn find ways to transcend them and foster international inter-network *communication* (Abbate, 1999, pp. 122-124). Although the Department of Defense stipulated communication as a primary objective for networking, the focus was on survivability to ensure national security. By contrast, Cerf and Kahn, among others, created TCI/IP to open gateways that would make it easier for different national networks to seamlessly interact and communicate each other.[34] Kahn and Cerf's development of TCP/IP facilitated the application of networks for communicative purposes that cybernetic theorists had long imagined. In fact, one of the most vocal proponents of inter-network communication was J.C.R Licklider, who had served as Director of the ARPA's Information Processing Technique Office (which oversaw the ARPANET project) during the initial phases of ARPANET development (Licklider, 1960, 1963; Licklider & Taylor, 1968). As Licklider himself has said: "I wanted interactive computing, I wanted time sharing. I wanted themes like: computers are as much for communication as they are for calculation" (Licklider interview by Asprey & Norberg, 1988).[35]

The move away from the 'restricted access' precepts that surrounded the Internet's initial development was not only visible in the consequences of endorsing the NWG and adopting TCP/IP. A third development fundamentally removed the authority of defence agencies over the network. As the NWG and the international-internetworking initiatives

[34] In Cerf's own words, in developing TCP/IP they intended to create a system in which "you couldn't tell … that you were talking through different kinds of networks" (qtd. in Abbate, 1999, p. 128).
[35] Licklider was particularly influenced by Norbert Weiner's work on cybernetics. In addition to injecting this cybernetic spirit into the ARPANET's development, he published articles advocating the ways in which computers would enhance human knowledge and communication. Amongst the most widely cited is *Man-Computer Symbiosis* (Licklider, 1960)

gained prominence, networking was less and less defined by its defence objectives. Even more, when the DCA separated the ARPANET from MILNET, it undermined the idea that the DCA would have a single network (ARPANET) managed for a single purpose (security). Instead, the DCA had effectively created the ARPANET as a civilian network. As a result, by 1980 computer science researchers in non-ARPA-affiliated universities began to question why they were being denied access to large mainframe computers and other resources for networking and related research in the computer sciences (Abbate, 1999, p. 183). Under the initiative of Lawrence Landweber, chair of the computer science department at the University of Wisconsin, several computer science faculties approached the National Science Foundation (NSF) with a proposal to create a network that would serve the larger computer science research community. A new network – CSNET (Computer Science Network) was developed, which in time was linked to the ARPANET. Its connections to the ARPANET created a single online community of computer scientists in the United States but, more significantly, also made the ARPANET, despite its continued oversight by the DCA, a *civilian* network in all but name (Abbate, 1999, p. 184).

With the growing demand for research-based internetworking, the NSF quickly broadened its support for networking beyond CSNET. In 1980 it applied for and received congressional approval to build new supercomputer centres with the aim of providing nation-wide access to them. Based on its educational mandate, the objective was to make the computers available to any scholar (and his or her students) who required the use of supercomputers in their research projects. Due to the expense of supercomputers, the NSF was able to build only five. Accordingly, in order to maximize access, it decided to build a network that would connect the computers so they could be accessed remotely from other

sites. The proposed NSFNET would be a layered system whereby a series of regional networks would be connected to a single computer centre, which in turn would be connected to the NSFNET backbone. The NSFNET was thus designed as an inter-network from the outset. But, unlike the DCA's concerns with national security and defence, the NSF's network was based on open research and education. As growing connections between CSNET and ARPANET expanded civilian use of the ARPANET, the DCA lost interest in maintaining it. Recognizing that the ARPANET had outgrown its use for defence research and that its technology was becoming obsolete, rather than reinvest in the ARPANET, in 1990 the DCA decommissioned it.[36] In effect, the NSFNET became the Internet backbone in the United States. With its growing connections to networks around the world, it also became the backbone for the emerging global Internet. Whereas authority for network management had once been defined by national security objectives and placed in the hands of defence agencies, the expansion of civilian Internet use, triggered by research and educational objectives, shifted networking authority to the NSF.

In summary, 'open access' emerged as an alternative method to manage internetworking through the endorsement of the NWG open decision-making process, the (mis)application of TCP/IP to promote cross-border inter-network communication, and the expansion of civilian researcher participation in Internet development. Perhaps the most dramatic of these developments was the creation of a new national network (NSFNET) explicitly geared toward civilian research and education. With the NSFNET's educational mandate, a civilian ethos was becoming visible as the new context for Internet governance. The combined effect of these developments removed any practical association of the

[36] Decommissioning the ARPANET did not also shut down MILNET. MILNET remained operational and continued to be overseen by the DCA. See discussion of the transfer to the NSF at: http://www.livinginternet.com/i/ii_nsfnet.htm (accessed 13 March 2008)

ARPANET with defence mandates. Although the tenor of 'legitimacy crisis' was not pronounced as panic, the legitimating power of sovereignty and its security impulses were called into question as the framework for managing and developing the ARPANET and, in time, inter-networking.

Although the *global village* was not specifically articulated as the guiding vision for these developments, its influence on the broader context of inter-networking development is likely found in the graduate students' approach to network management. Transcending borders and enhancing communications rather than protecting borders and limiting communications within a particular geographical space, as TCP/IP developed alongside the practices of the NWG, the evolving Internet's 'global' scope was developing through anti-hierarchical, deliberative, inclusive processes of decision-making by a dispersed set of network managers and civilian users. Networking research and even inter-networking communication may have begun as a sovereign enterprise directed toward national defence but it was slowly moving toward a global project underwritten by more placid intentions. The new terminology for the Internet makes this intention evident, especially in attempts to open access: for instance, *decentralization*, *user-empowerment*, *open architecture*, and *communications*. While the advocacy of 'open access' by an academic community is not surprising, during this period it seems to be inflected by the normative flavour of the cybernetic *global village*. The misappropriation of McLuhan's *global village* by the countercultural movement and its convergence with the open dialogue favoured by ARPA graduate students appears to have influenced a misappropriation of the ARPANET's objectives and management culture – 'command and control' were being disrupted by communication and collaboration.

Incorporating the political vocabulary of 'open access'

If legitimacy crises set the scene for the incorporation of a new political vocabulary that redefine the 'facts' of political order, the NWG's open standards process, the application of TCP/IP to promote inter-network communication, and the shift of authority to the NSF's civilian research and education mandate created the conditions for the adoption of *decentralization*, *user-empowerment*, *open architecture*, and *communications* as the new vocabulary for Internet governance and, as a result, 'open access' as the legitimating principle of Internet governance. Given the shift towards user-driven and research mandates for networking research and development, the efforts of the computer science/technical community and the NSF became the central locus in the attempt to redefine the Internet beyond its security-driven applications. This effort entailed defining the Internet as a global, user-oriented, public, communications medium. Inspired by TCP/IP's 'borderless' communications architecture, incorporating 'open access' had the effect of expanding Internet use to civilian users in the United States and users around the world. The legitimation of 'open access' as a principle for Internet governance therefore globalized the Internet by putting a priority on expanding the Internet to promote open communications around the world. User-driven development became the overarching governance objective of the emerging global Internet. To the degree that 'open access' was influenced by the *global village* metaphor, the incorporation of this new vocabulary and the 'facts' it established reflect the way the normative tenor of the metaphor was inscribed into the evolving framework for global Internet governance.

The ‘open access’ vocabulary was incorporated in two parallel developments. The first involved the implementation of the NSF’s policies around the use and expansion of the NSFNET among its emerging worldwide constituency of users. As a response to the exponential growth of worldwide Internet activity triggered by the growth of the NSFNET, the second related to ARPA’s creation of a mechanism to allow the growing worldwide user community to be involved in discussions about developing Internet standards. Both converged when the NSF privatized the NSFNET backbone. Leaving Internet users in charge of standards making, the conditions were set to incorporate a vocabulary that fostered the development of a global system for Internet governance.

Building the global civilian Internet: the NSF’s Acceptable Use Policy

The changing context of Internet governance was perhaps most visible in the transfer of authority from US defence agencies to the NSF. Whereas ARPA principal investigators in the 1960s had defended networking research in military terms to Congress, the decision to build NSFNET meant that Congress was now pushing networking in research and educational terms.

Section 3a(4) of the National Science Foundation Act of 1950 gave the NSF the authority to “foster and support the development and use of computer and other scientific and engineering methods and technologies, primarily for research and education.” It was on this basis that Congress approved the NSF’s involvement in networking research (Office of the Inspector General, 1993). Under the NSF, the normative ethos of the Internet was transformed from the need to ensure survivable communications for national security to

communications that "[supported] open research and education in US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication."[37] This new approach to managing the Internet was principally articulated and disseminated through the NSF's *Acceptable Use Policy* for NSFNET.[38] Although the focus on research and education in US educational institutions appears to be a set of limitations – that is, by applying to US users only and the priority placed on research application, the *Acceptable Use Policy* actually expanded the Internet's user-base beyond the territorial borders of the United States.

First, and foremost, because of its focus on research and education, the NSF promoted universal educational access. It thus enhanced greater public use of the NSFNET by funding campus connections across the US, with the strict requirement that universities ensured that their employees and students (and in some cases members of the local community) would all have access to the network, usually in the form of an email account (Krol & Hoffman, 1993).

Second, universal educational access was enhanced when the *Acceptable Use Policy* prohibited use of the NSFNET for "for-profit activities," for "personal and private business" and for "advertising of any kind."[39] According to Misa (2004, p. 253), by banning commercial use of the network, the NSF "reinforced the idea that [the Internet] was a *free* collection of individuals" (my emphasis). From a user perspective, the Internet was free of charge. Preventing commercial use intended to keep the Internet a non-proprietary space.

---

[37] Principle 1 of *The NSFNET BACKBONE SERVICES Acceptable Use Policy* Available: http://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt (accessed 6 July 2007).

[38] Available: http://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt (accessed 6 July 2007)

[39] Principles 7, 10 and 11 of the *NSFNET BACKBONE SERVICES Acceptable Use Policy* respectively stipulated that acceptable use of the network included "Announcements of new products or services for use in research or instruction, *but not advertising of any kind*" (Article 7) and that "Use of for-profit activities unless covered by the General Principle or as a specifically acceptable use" and "Extensive use for private or personal business" as unacceptable uses. Available: http://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt (accessed 6 July 2007).

Geared toward education and research, access should be universal rather than determined by the ability to pay (Krol & Hoffman, 1993). Although a review of the NSFNET in 1993 granted access to commercial traffic, it was permitted only in circumstances in which it enhanced scientific research and education (Office of the Inspector General, 1993).

Third, the *Acceptable Use Policy* promoted global connections. Initially this was a response to demands by US researchers, who pointed to the NSF mandate to promote dialogue between US and foreign scholars. The enthusiasm among US researchers and the way research was conducted between scholars in different parts of the world therefore contributed to the expansion of the NSFNET outside US territorial borders. However, expanding the NSFNET faced two obstacles. First, the NSF feared that connecting it with civilian networks in other countries would be seen as "the encroachment of US networks [and] a form of imperialism" (Abbate, 1999, p. 209). There was also a chance that US citizens would perceive this kind of expansion as giving away a US-tax-payer-subsidized resource. Thus, at the outset, other networks such as USENET and BITNET, grew faster than the Internet. Because the NSF was not bound by the military's restrictions on allowing connections from other countries, the NSF enhanced the NSFNET's, and thereby the Internet's, global potential by allowing foreign networks to connect to the NSFNET (Abbate, 1999, pp. 208-209). By the mid-1980s, because of the tremendous resources dedicated by the NSF to internetworking, other national academic research networks from Canada, Europe, and Asia began building gateways to connect to the NSFNET backbone. Between 1990 and 1995, the number of non-US networks connected to the NSF grew from 20 to 40 percent (Abbate, 1999, pp. 208-209; Randall, 1997), rendering obsolete the notion that the Internet was an American national project. Although the NSF's *Acceptable Use Policy* was in

principle limited only to networks and users in the United States (because many networks from different parts of the world connected to the NSF backbone), these other networks were also bound by the rules and regulations stipulating 'appropriate' use (McTaggart, 2004, pp. 137 - 140).[40] As a result, the *Acceptable Use Policy* indirectly became *the* policy for the evolving global Internet

Underwriting all the other changes, the *Acceptable Use Policy* emphasized the use of the NSFNET for communication between *people*. Although the idea of an Internet based on communications was evident in the motivations behind the TCP/IP protocol, with the public access initiatives supported by the NSF, the Internet became associated with – indeed celebrated for — facilitating people-to-people communications, primarily as a result of the widespread use of email. Although email was a peripheral application in the ARPANET's early design, it became the dominant reason to use the ARPANET. Email allowed researchers from distant computer sites to communicate more easily with each other, and with the invention of mailing lists, with the entire group. Not only did ARPANET researchers note the importance of email in developing the ARPANET, they noted the ways in which email developed a sense of community among ARPA members. They sensed that this 'community-building' aspect had tremendous potential outside of its limited use among researchers. As two ARPA members noted, "We in the ARPA community … have come to realize that we have in our hands something very big, and possibly very important. It is now plain to all of us that message service over computer networks has enormous potential for changing the way communication is done in all sectors of our society: military, civilian government, or private" (Myer and Dods qtd. by Flichy, 2007, p. 47).

[40] This did not preclude commercial activity per se on connecting networks, but it did act as a hindrance if they were to be connected to the NSFNET.

More than just the ability to correspond with family, friends, and colleagues without the restrictions of time and space, email played a direct role in creating 'on-line communities,' where individuals worldwide, with no previous personal connection, would congregate to discuss any number of topics. The Internet's virtual communities thus gave expression to cyberlibertarian and cosmopolitan aspirations that the Internet would promote a new kind of social space – cyberspace – that transcended national identities, free from the coercive authority of governments. Widespread use of email also contributed to the Internet's depiction as a deliberative public sphere that encouraged the communication and understanding between individuals and cultures that physical distance made difficult or even undermined (Flichy, 2007; Godwin, 2003; Valovic, 2000). To a significant degree, then, the popularity of email made the Internet emerge and gain public prominence as a *global village*.

Through the *Acceptable Use Policy* 'open access' was incorporated as a principle for managing and using the Internet by directing the network toward *civilian* and *public* uses and fostering a sense of *people-to-people communication* within a *non-commercial* and *non-proprietary* context. It was not simply about enlarging the number of US users, but developing a communications capacity on a global scale. When asked whether the growth of the NSFNET was "contributing to [the emergence of a] global village?", Steven Goldstein, the NSF's program director for interagency and international coordination in the mid-1990s, answered, "It already [had] … [With the Internet] you can be part of a community without any national borders… Where we happen to be physically is unimportant; we're just part of that community" (qtd. in Stilkind, 1996).

Building the global Internet community: the emergence of the IETF standards-making process

Parallel to and in part enabled by the greater civilian use of the ARPANET, the eventual transfer of civilian networking authority to the NSF and the emergence of NSFNET as the Internet backbone involved a series of debates among computer scientists and engineers about how to bring in the growing global constituency of users. Because the Internet was still in its formative stages, these discussions revolved around how to include users in decisions about which standards to adopt for the Internet (Drake, 2004, pp. 123-124; Goldsmith & Wu, 2006, pp. 23-24; Hofmann, 2005; Lessig, 1999, p. 207; Mueller, 2002, pp. 39,73). Evidently, this effort was a continuation of the NWG's emphasis on a user-driven approach to developing standards for the ARPANET. However, while the NWG's process remained within the scope of governmental authority, even while undermining it, the evolving user community interpreted the Internet's open architecture principle and its user-empowerment principles as a need to move standards-making out of government hands. On the one hand, this was a direct challenge to the US government, as the number of non-US users was rapidly growing. On the other, based on governments' top-down bureaucratic approach to decision-making, it was a rejection of governmental authority outright. 'Open access' was therefore both a means to expand standards development beyond its association with the US government and also a way to create a *decentralized*, *bottom-up*, *user-driven*, and *deliberative* standards process. The IETF emerged in this process. However, the vocabulary itself does not fully account for why the IETF was eventually considered the embodiment of

the *global village* metaphor in global Internet governance. How this happened will become clearer later in the chapter.

The first phase of breaking the relationship with government had to do with the US government's formal authority over the evolving Internet and users' desire to devise the Internet's technical standards independently. Although in 1984 ARPA responded to the tremendous growth of worldwide Internet activity by creating the Internet Activities Board (IAB) and invited users, network managers, and anyone from anywhere in the world to participate in discussions and decisions about internetworking, the process was still formally overseen by ARPA, a US federal agency. When in 1986 the IAB was restructured into a series of task forces, the IETF emerged as the locus for developing the evolving Internet's day-to-day technical standards. As the IETF conducted its discussions about the Internet's technical design according to an ethos similar to the NWG's (given that many of its key participants were former NWG members), extending it to a growing worldwide community, its participants began to assert that the authority for creating Internet standards lay in the hands of the global community of Internet users rather than any particular government. Even with these claims, and evidence that the Internet could not be located in any single national jurisdiction, the history of the Internet's development in the US continued to tie the IETF to the US government. It was thereby still required at some level to "conform at least loosely to its federal paymaster's needs" (Froomkin, 2003, p. 786) (c.f. Cerf, 1989). This left the IAB and the IETF in particular in the paradoxical position of trying to assert the independence of the global community of Internet users as the legitimate site of Internet standards-making, while formal authority remained in the hands of a single federal government.

Although the transfer of authority to the NSF did dislodge the security mandates for networking development, management remained in the hands of a US government agency, and the IETF still officially operated under ARPA. However, the IETF forged a relatively uncontroversial relationship with the NSF. In fact, the NSF deferred to the 'authority' of the IETF. One former NSF official described the IETF has an "enlightened monarchy in which the federal government funded the best brains. Their output was RFCs, which were approved through a collegial, though sometimes brutal process of someone advancing an idea and everyone beating on it until the group consensus was that it would work" (Mitchell qtd. in Mueller, 2002, p. 94). Thus even though RFCs lacked a formal legal basis, the IETF process through which they were forged were for the NSF "the way reality was defined on the Internet" (Mueller, 2002, p. 93). With this endorsement, the IETF increasingly began to describe itself as an independent and "unincorporated, volunteer organization, with support to participating individuals/organizations from the US government or from the individual's own organization" (Cerf qtd. in Mueller, 2002, p. 93). This was not a rejection of governmental involvement altogether. Structuring the process around the IETF's bottom-up, deliberative approach to standards-making during this phase simply moved the US government from being the principal site of standards-making to a partner that supported and encouraged the "working anarchy" of the growing global user constituency (Mitchell qtd. in Mueller, 2002, p. 94).

However, adopting the government as a partner was soon rejected. The second move towards 'open access' occurred when the IETF abandoned its association with the International Standards Organization (ISO). Operating with greater independence, the IETF sought to professionalize its activities by coordinating its standards discussions with

networking projects taking place at the ISO. As a non-binding *inter*-national treaty organization overseeing a number of voluntary international standards, the ISO appeared to be an attractive partner. The ISO was also actively involved in developing inter-networking standards. In 1978 it proposed the development of the Open Standards Interconnection Basic Reference Model (OSI) as the new universal networking standard. OSI did not seek to replace TCP/IP as such, but to create a meta-structure in which TCP/IP would be one of many network layers.

OSI was forged by governments' desire to ensure the Internet developed according to open and non-proprietary standards. Frustrated by the development of proprietary standards for internetworking by IBM, Digital Equipment Corporation, and Xerox, who refused to make the standards compatible with competing systems, governments took the initiative to create non-proprietary network protocols (Abbate, 1999; Drezner, 2004, pp. 491-492). The first of these, X.25, was developed by the Canadian, British, and French governments and was adopted by the ITU in 1976. The adoption of X.25 in key markets – France, Britain, and Japan – put pressure on corporate actors to make their proprietary standards compatible with X.25. As Abbate (2001, p. 163) concludes, "X.25 was explicitly designed to alter the balance of power … and in this it succeeded. Public data networks did not have to depend on proprietary network systems from IBM or any other company." OSI was promoted with similar objectives. As an open standard, it would be available to anyone who wished to implement it and, developed by the ISO, it would be managed by a public rather than private organization (Abbate, 1999, pp. 166-167). Western countries, where network technology was most developed, enthusiastically endorsed OSI. European governments voiced their support because it provided a way for the European computer sector to compete with American

corporations, who were at the time dominating the market (Abbate, 1999, pp. 171-172). The US government advocated its support because of its preference for non-proprietary and open-source standards (Drezner, 2004, p. 492). With the ISO's emphasis on non-proprietary standards, IETF users shared with it a common objective. However, in contrast to the IETF's bottom-up process of testing, implementation, and then standardization, the ISO opted to perfect OSI and then offer it to users as a standard to be implemented. For IETF members, this prescriptive approach raised serious questions about whether OSI would even work. OSI nonetheless continued to receive widespread government support. As discussions continued, the IETF felt that governmental agendas and preferences for top-down management were compromising the Internet's technical integrity (Abbate, 1999, pp. 171-177; Drake, 1993; Randall, 1997, p. 207; A. L. Russell, 2006).

More than a technical concern triggered IETF participants' consternation. Their anger toward the OSI's prescriptive methodology was also motivated by a deeper normative commitment to user-empowerment. If governmental efforts had reinforced 'open access' by promoting non-proprietary standards, their approach to standards undermined it. By precluding user testing and implementation, the ISO not only contested the principle of user-empowerment at the core of the network's technical architecture — it also contravened the growing perception among IETF participants that user-empowerment was the political principle of Internet standards making. As one IETF participant commented, "*Internet* standards tended to be those written for implementers. *International* standards were written as documents to be obeyed" (Mills qtd. in A. L. Russell, 2006, pp. 53-54). If the IETF at first rejected government as an overseeing authority but accepted it as an equal partner, after its

experience with the ISO, users argued that governments should be denied any role in the development of Internet standards (Drake, 1993; Hofmann, 2005; A. L. Russell, 2006).

By 1992 frustrations with the ISO process led the IAB and IETF to professionalize their activities under the umbrella of a new organization, the Internet Society (ISOC). Shedding any association with government, ISOC was founded with the mission to "promote the *open* development, evolution and use of the Internet for the benefit of all *people* around the *world*" (Internet Society, 1992; my emphasis). However, it was only in 1995 that this mission was legitimated and the IETF's desire to prohibit governmental involvement really bore fruit. In that year, the NSF privatized the NSF backbone, which meant that standards making also had to move outside of the US government's purview. As OSI had failed to achieve widespread acceptance and implementation, the IETF and its global community of users were *de facto* authorized to develop Internet standards. As the new authoritative locus of Internet standards making, the IETF seemed to achieve its goal of "[denying] governments the right, and above all the ability to develop suitable and legitimate governance structures for the Internet" (Hofmann, 2005, p. 9).

Drezner (2004, p. 493) argues that because governments had already expressed a preference for TCP/IP, regardless of the failure to adopt OSI and the ISO process, TCP/IP's success is evidence that the development of the Internet was ultimately directed by states, which delegated their authority over standards making to the IETF. Sovereign authorities rather than the technical community directed Internet governance. However, the rejection and ultimate removal of governmental involvement from the standards process suggests that the power to implement TCP/IP as a standard lay in the hands of the technical community. While states and the technical community converged around TCP/IP as the appropriate standard for

communications, convergence between state interests and the technical community alone is insufficient to measure sovereign power. Given state support for OSI as the overriding protocol suite, the failure to adopt OSI suggests that state preferences were in fact marginalized as the Internet developed. One can therefore surmise that TCP/IP provided an adequate and functional solution to states' preference for non-proprietary Internet standards. At most, convergence explains why there was little government resistance to the emerging authority of the IETF rather than evidence that states directed the process. In fact, through the privatization of the NSF backbone, the United States somewhat removed itself from the development of Internet standards.[41] In light of the failure of OSI to gain acceptance, the ISO faded into the background.

With governments – both US government agencies and the ISO – removed from the actual work of devising Internet standards, the IETF could implement the 'acceptable policies' for the standards-making process. Unsurprisingly, it was at this time that the incorporation of a new vocabulary globalizing the Internet and its governance was most explicit. Because the Internet's governance largely revolved around developing technical standards, the new political vocabulary was most visible in the texts outlining the requirements for the IETF's standards process (D. Crocker, 1993; IETF Secretariat, CNRI, & Malkin, 1994; Internet Activities Board, 1992; Internet Architecture Board & Internet Engineering Steering Group, 1994; G. Malkin, 1993).

The process itself was open to anyone with the time and willingness to participate. With an emphasis on *accessibility*, discussions and definitive decisions were made in a *decentralized* fashion in *user*-driven working groups conducting their discussions on

[41] The US government still had authority over certain technical features of the Internet – specifically the rootzone file. See Chapter 2.

electronic mailing lists to allow for remote participation. Consequently, decisions were never made at any of the IETF's face-to-face meetings – which were intended to be more informational – they had to be 'taken to the list' (Bradner, 1998, p. 12). Moreover, all standards were *voluntary*. Even if standards enjoyed widespread support from the IETF's technical community, individual network managers could choose not to adopt them. Of course some standards were 'required.' For instance, without TCP/IP, one would not be able to communicate with other networks. However, no standards were ever deemed mandatory. Even if "Requests for Comments" or RFCs were now official standards documents, they were only *de facto* standards. Because IETF participants tended to view the Internet and its resources as held in common, all standards were *non-proprietary*. A poster tacked onto a computer administrator's door in 1991 summarizes the prevailing attitude at the time: "The Internet is like an ocean. It is a great resource. It is huge. No one owns it" (qtd. in Mueller, 2002, p. 57). The IETF therefore emphasized that all contributions to standards were made for the good of the Internet, not for individual gain (TAO of the IETF). As David Crocker (1993, p. 52) summarized, "making standards the IETF way" stressed "people, not procedure" (in contrast to the ISO), "diverse contributions," "online collaboration," and "easy to access standards" (non-proprietary and free).

The most distinctive feature of the IETF standards process was its *deliberative* approach. Of course the ultimate test for a standard was its technical feasibility. However, demonstrating this feasibility was not a matter of taking it to a vote. Harkening back to the NWG process, the IETF worked toward consensus. This did not mean that everyone was always happy, but it did remove the 'tyranny of the majority' that could leave some users isolated and marginalized. As defined by the IETF itself, "51% does not qualify as 'rough

consensus' and 99% is better than rough" (Bradner, 1998, p. 13). Combined with the commitment to open membership and process, 'rough consensus' usually meant that a proposed specification already had widespread public support when it was approved as a standard, rather than demanding support after the fact.

In summary, the 'open access' political vocabulary inspired by the *global village* metaphor was incorporated in two mutually forcing steps. First, the transfer of authority from the DCA to the NSF over the Internet and the NSF's ability to enforce its *Acceptable Use Policy* fostered an Internet defined as a *global*, *civilian*, *non-commercial*, *people-to-people communication*s medium. Second, and in part enabled by the first, the authorization of the IETF and its globally dispersed set of users as the appropriate progenitors of Internet standards instilled the terminologies of *open process, accessible, voluntary, non-proprietary, bottom-up, user-driven, deliberation* as the framework for how the Internet standards process, and by extension global Internet governance, was defined. In short, the NSF and IAB-IETF efforts mutually reinforced 'open access' as the description of the Internet and also the legitimating principle by which it was to be governed.

The juxtaposition of the *global village* metaphor's vocabulary with discourses of sovereignty was evident in the challenge posed to 'restricted access' principles. As networking went beyond 'national security,' the category of users was expanded to include the broader public, first in the United States, and then around the world. Additionally, through rejection of the ISO process, the 'rough consensus' approach of the IETF defined users not only as 'implementers' of the Internet and its technical requirements but also its 'creators.' By the time the IETF standards documents were circulated, it was clear that the *global*, *open*, *bottom-up*, *grassroots*, *deliberative* were championed over the *national*, *closed*,

hierarchical, *top-down* structures of the ARPANET and its association with doctrines of national security and defence. In other words, when the Internet was no longer a project of national security but a project of open communication it was no longer subject to the top-down directives of government bureaucracy.

This displaced the legitimating power of sovereignty by eliminating survivability as the goal of network development and removing government as an agency – both through its directives and also its functional involvement – from the standards-making process. Despite the IETF's interaction with the ISO, the progressive removal of governmental authority was not always the result of the user community's hostile rejection of governments. By promoting the NSFNET as a universal, public communications medium, the NSF, a US government agency, contributed to the development of the Internet's global support. It ensured that the NSFNET was available to users worldwide. Moreover, the NSF's endorsement of the IETF likely allowed for its emergence as the *de facto* home of standards-making after the NSF backbone was privatized. Although the Internet's origins were national security, the evolution of its networking towards open, civilian, and communicative ends promoted a global Internet and its worldwide governance. These developments support Sassen's (2006) observation that key 'triggers' for globalization often occur through a series of denationalizing policies and processes located deep inside the national domain.

The territorial limits of the Internet were further removed once the vocabulary of communications between networks instilled the idea of a worldwide user community. In this way the *state of nature* metaphor's emphasis on states as persons was undermined as individuals or the global 'Internet community' became the relevant people served by inter-networked communications. If globalization is a *normative* vocabulary of deterritorialization

that constitutes a particular system of global governance, the influence of the *global village* metaphor through the principle of 'open access' deterritorialized the Internet and its governance by removing the 'command and control' doctrines of sovereignty by promoting principles of open use, participation, and deliberation.

Hoffman argues, "What characterized the IETF was not only its technological know-how and eagerness to innovate but also its rather academic structure, which was intentionally fashioned as an alternative to state and intergovernmental standards organizations." Thus, to the degree that the IETF's vocabulary for Internet governance reflected the influence of the *global village* metaphor, it was through the continuing influence of the NWG's approach to networking governance, evident in the involvement of NWG members in the IETF. However, by the early 1990s, 'open access' was no longer a disruption of existing 'facts,' as it had been in the early 1970s, but the normal and expected way to speak about managing the Internet. The legitimating power of the metaphor was emerging as a new set of logical answers was being established for how governance should be organized. Specifically, 'open access' became the 'why,' Internet technical standards development the 'what,' the global 'Internet community' of users the 'who,' rough consensus and deliberation the 'how,' and IETF mailings lists and working groups the 'where.'

Defining roles and responsibilities: 'open access' and the Internet community's network of action

'Open access' authorized the Internet user community in the form of the IETF as the appropriate site for making standards decisions. Once governments were removed from the

standards process, the IETF eventually became the venerated institution – the 'where' – for the evolving system of global Internet governance (Goldsmith & Wu, 2006, pp. 23-25). But before the IETF assumed its prominent status, the user community itself had to ensure that 'open access' was the guiding principle of the Internet standards process. Because the IETF was established as a task force of the IAB, the IAB had final authority over all standards decisions. Effectively, this meant that although users did the actual technical work to devise standards through participatory processes, decisions were ultimately made by a small self-selected group of ARPA veterans. Unsurprisingly, as 'open access' was being incorporated to define the Internet, it created tensions between the IAB and the IETF. The resolution of these tensions put decision-making authority in the hands of IETF participants. This change sheds light on how a vocabulary of *user-empowerment*, *participatory*, *decentralized*, and *bottom-up* standards making was establishing the terms of reference for governance and shaping specific actions and institutions. In the case of the Internet user community, the incorporation of 'open access' redirected the roles and responsibilities of the IAB and IETF, and put the IETF at the forefront of global Internet governance.

The hierarchical authority structure in the IAB and IETF relationship looked like this: Once a specification received the consensus of an IETF working group, the proposed standard was submitted to the Internet Engineering Steering Group (ISEG),[42] who put the standard before the IETF membership for final deliberation and review. Based on the results of that process, the IESG would decide on whether to pass on the proposed standard to the

[42] As the IETF grew in size, the number of issues to address grew astronomically. Working groups were accordingly organized within a number of functional areas considered to cover most of the short-to-medium-term issues regarding Internet architecture. An Area Director was appointed to each functional area in order to keep track of the discussions taking place in different working groups. The Internet Engineering Steering Group (IESG) was created to allow different Area Directors to communicate with each other and ensure that the proposal made by different working groups were technically compatible.

IAB for final approval. If approved by the IAB, it would be declared an official (although voluntary) Internet Standard (Internet Activities Board, 1992).

In practice, this process entailed a bottom-up, user-driven approach to developing standards. In principle, however, the IAB stood above the IETF as a review body with veto power over the acceptance or rejection of standards. RFC 1310, which delineated the standards-making process, stipulated that the IAB "delegated" the "primary responsibility for the development of and review of potential standards" to the IETF but that the IAB made "final decisions about Internet Standardization" (Internet Activities Board, 1992, p. 3). To the degree that the IAB did consult with the IETF, the deliberations were limited to asking a particular working group to clarify aspects of an approved standard or to reconvene and implement a recommendation suggested by the IAB (Internet Activities Board, 1992, p. 8). Effectively, then, what was meant to be a horizontal distribution of power among individual users was actually institutionalized as a chain of command in which the IETF was subject to the IAB's supervision.

The IAB-IETF relationship was thus not an immediate reflection of the power and legitimacy of the 'open access' principle. As a self-selected group of individuals who had been involved in the ARPANET, the IAB with its hierarchical authority over the IETF appeared to be a relic of 'restricted access.' Although no longer formally funded by or contracted by defence agencies, the top-down approach seemed to invoke the priority of defence officials and contracted parties over civilians by suggesting that the experience of IAB members in developing the ARPANET gave them certain privileges. According to Mueller (2002, p. 92), IETF participants saw ARPA veterans as an 'old boys' network who "stood at the top of [an] informal pecking order."

If the IAB had by and large accepted the IETF decisions, with its approval serving only as a formality, frustrations might have been held at bay. In June 1992, extended IETF discussions over how to solve the problem of the depleting Internet address space failed to produce a solution. Concerned by the lack of progress, the IAB made an executive decision, outlining a specific solution that it hoped would force the IETF to move forward. IETF participants widely condemned the memo. Despite all their misgivings about the process, the IAB still 'delegated' the actual discussion of the technical features of standards to the IETF. The memo was therefore interpreted as an attempt to undermine the way in which the IETF could actually, even if imperfectly, contribute to standards-making. As one commentator described the IAB's actions, "this was at best drafting, not reviewing; at worst it was usurpation" (Froomkin, 2003, p. 789) (see also S. Crocker, 1994, pp. 1-2). From the IAB's perspective, the memo was meant as only a proposal to offer advice rather than impose a prescriptive solution (S. Crocker, 1994, p. 1). But for IETF participants even putting forward a proposal was an attempt to take over their role in the standards process. As one participant recalls, "The June communication from the IAB was understood by many [as] an IAB decision, or equivalently, a sense of the decisions the IAB would make in the future" (S. Crocker, 1994, p. 1). Crocker (1994) argues that the entire controversy was based on a miscommunication. When there was a smaller user community, IAB members were in close communication with IETF working groups. However, with the rapid growth of the Internet, it was becoming more and more difficult to maintain direct contact with the burgeoning IETF user community and all of its different working groups. According to Russell (2006, p. 48), the 1992 miscommunication was evidence that "IAB and IETF started to become victims of their own success and [were struggling] to preserve their founding principles."

The perceived usurpation was made even worse by the actual content of the memo. Not only was it considered technically unsound, it also proposed adopting part of the ISO's OSI model for the Internet address space. Given the hostility toward the ISO among IETF members, any association with the ISO was considered "rank heresy" (Cargill qtd. in Drake, 1993; A. L. Russell, 2006). To defer to the OSI model bolstered the view among IETF participation that the IAB-IETF relationship was increasingly at odds with the user-driven deliberative processes the IETF valued, which had been the basis for the user community's controversial break with the ISO (A. L. Russell, 2006).

Aggravation increased in the few days following the memo. The IAB announced that as a result of its association with ISOC it was changing its name from the Internet *Activities* Board to the Internet *Architecture* Board. The change was meant to reflect the IAB's new role as ISOC's technical *advisory* committee. The IAB hoped to emphasize that it had a role only in overseeing the evolution of the Internet's architecture and did not directly participate in the development of technical standards – which was the responsibility of the IETF (Froomkin, 2003, p. 789) (c.f. D. Crocker, 1993, p. 50). However, in light of the prescriptive memo, the IETF interpreted the IAB's inclusion of 'architecture' to suggest that the IAB no longer considered the IETF qualified to oversee the Internet's architecture and thereby diminished its role in the standards process ("The 2nd Boston Tea Party", 2000). All in all, the memo, and the events surrounding it, appeared from the IETF point of view as a way to deepen the IAB's authority over the IETF and the standards process. If the global Internet user community, represented by the IAB and the IETF, had been legitimated as the authoritative site of standards-making when the vocabulary of 'open access' was incorporated into discussions about Internet governance, the memo put this vocabulary's

legitimacy into crisis along with the principle of 'open access' (Froomkin, 2003; A. L. Russell, 2006).

IETF participants began to question whether their relationship with the IAB was at all useful. Feeling misunderstood, IAB board members, in particular Vint Cerf and David Clark, addressed IETF participants at the next IETF meeting. They hoped to allay their fears and assure them that in fact the IAB valued the IETF's user-driven process both as a matter of ensuring technical feasibility and also as the ethic of standards-making (A. L. Russell, 2006, p. 55). Clark (1992) argued that the IAB was committed to the following credo: "We don't believe in kings, presidents and voting: we believe in rough consensus and running code." The 'rough consensus' model, he argued, was superior to the ISO's weighty bureaucratic process and the IETF's approach to 'running code,' which prized testing and user implementation, was the optimal way to devise Internet protocols. According to McTaggart (2004, p. 234), "by saying that the IETF community rejects kings and presidents, Clark was reassuring the rank and file that there was no secret cabal (as some had accused the old IAB of being) in control of the IETF … The catchphrase means that if someone can demonstrate a working prototype, and if rough consensus emerges on the suitability of its design, then the recognition of the community is all it takes to make it 'official,' not the blessing of any political or corporate authority." In short, Clark presented 'rough consensus and running code' not just as a way to describe the technical value of the standards process but more importantly as its founding political principles.

Despite IAB efforts to stress its allegiance with the IETF, IETF members were still unsatisfied. They thought 'rough consensus and running code,' was not in the least an apt description of how the standard process actually worked. If these were the founding

principles, then much had to be done to (re)embed them in the process. IAB attempts to clarify the memo as only a proposal and *not* as a prescription did little to calm the IETF who felt the IAB had failed to address broader dissatisfaction with its hierarchical authority. Cerf and Clark's comments therefore further galvanized the IETF. Rather than rallying around 'rough consensus and running code' *with* the IAB, IETF participants seized upon it as a way to call the IAB to task and reform and restructure the standards-making process.

Principally, then, the IETF embarked on a task to redefine roles and responsibilities so that the Internet standards-making process would reflect 'open access' as the legitimating principle. They formed a working group – the Process for Organization of Internet Standards (POISED) Working Group – to address "to what extent should the [IAB] make decisions and to what extent should it provide technical guidance?" (S. Crocker, 1994, p. 1)[43] The working group therefore was not a discussion about a technical specification but about the legitimate process through which technical standards were made.

POISED recommendations radically redefined the roles and responsibilities of the IAB, IESG, and the IETF and their overall relationship to each other. IETF working groups would remain the homestead of technical discussions, user testing, and implementation. However, the IAB would no longer have final authority over IETF decisions. Instead, the IAB would adopt only an oversight role over the entire process, with "all processing of standards actions, including the final decision to advance a specification along the standards track … made by the IESG" (S. Crocker, 1994, p. 3). In short, *users* would not only create standards — they would accept or reject them.

[43] POISED also addressed the question about how members for the IAB would be selected and length of terms for IAB members. Due to its preference for consensus over voting as a more democratic process, it resulted in the creation of a sophisticated series of nominating and selection procedures (see S. Crocker, 1994; Galvin, 1996).

The challenge would be to bring IAB members on board which proved to be less difficult than expected. Because many IAB members had been involved in designing the NWG's radical approach to standards making, IAB members were just as concerned about the fracturing process and responded with a set of proposals that supported POISED recommendations: *all* decisions, including the final decision, regarding technical requirements would be made by the IESG (S. Crocker, 1994). The IAB would step in only if there was a dispute between IETF participants and the IESG – as a last resort. In this new role, the IAB would be an appellate body that would step in and mediate disputes. The proposal from the IAB moved the IAB and IETF closer to consensus. As Crocker (1994, p. 3) describes it, "convergence on this key point obviated a radical proposal and signaled the building of a consensus on how the standards process should evolve."

The consensus was evidence of a new alliance of interests reflected in the revised standards procedures, RFC 1602 — "The Internet Standards Process – Revision 2" (Internet Architecture Board & Internet Engineering Steering Group, 1994). In contrast to the original standards process in which the IAB 'delegated' authority to the IETF and held 'final authority' over standards decisions, RFC 1602 described the standards process as "allowing the *general* Internet community to show preferences by making its *own* choices, rather than by having legislated decisions" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 24).

The IAB's new role determined how the activities of the IETF and IESG were restructured. With the IAB now defined as a "body to which the decisions of the IESG may be appealed," gone was the notion that Internet standards were made by a small, self-selected group (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 7).

Instead, the IESG was made "directly responsible for the actions associated with entry into and movement along the 'standards track' … including the *final approval* of specifications as Internet Standards" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 7; my emphasis). This did not replace the hierarchical relationship between the IAB and IETF with a new one between the IESG and the IETF. Rather the IESG made its decisions based on widespread consultations with IETF participants. After a proposal was submitted, and area directors agreed that it met the necessary technical specifications, the IESG was required to "permit final review [of a proposed standard] by the general Internet community." This differed vastly from the IAB approach of closed discussion, with consultations conducted only to get clarification or have the working group reconvene to implement a recommendation (c.f. Internet Activities Board, 1992, p. 8). Altogether, these changes restructured the standards-making process so that the IAB was no longer the "primary coordinating committee for Internet design, engineering and management" (Internet Activities Board, 1992, p. 3). The revised standards process stipulated that the IETF was "the *principal* body engaged in the development of new Internet Standards specifications," which referred both to the actual production of technical codes and the deliberations over whether to accept or reject them (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 7; my emphasis).

Because the IAB's oversight and appellate role gave decision-making authority to users, it brought to life the idea that 'rough consensus and running code' are both a matter of technical feasibility and a way to promote and foster user-driven, bottom-up, deliberative participation. It facilitated the connection between technical process and political legitimacy by putting the creative work in IETF working groups and final decision-making authority in

IESG. While each group – the IAB, the IESG, the IETF – operated with their own specific functions and set of tasks (their localized roles), the collective outcome of these roles established the IETF and its working groups as the appropriate decision-making locus of the standards process. The legitimating power of 'open access' was therefore evident as the concrete actions of different groups collectively produced an anti-hierarchical and participatory political order.

With the IETF now considered the 'principal body' for standards making, it no longer supported the activities of the IAB. Instead, the IAB supported the work of the IETF working groups – and only 'as a last resort.' The consolidation of the standards process around IETF working groups was made evident by RFC 2028, which was called the "Organizations Involved in the *IETF* Standards Process" (Hovey & Bradner, 1996; my emphasis). Referring to the standards process in a way that gave prominence to the IETF did not diminish the significance of the IAB and the IESG in supporting the IETF, but it did eclipse their specific functions. As 'open access' came to structure the Internet's political order, the prominence accorded to the IETF signified that it had become the 'black box' and thus an Internet governance institution.

The IETF also became the central reference point for Internet governance in the popular press. Catching the attention of *Wired* Magazine, perhaps the authoritative source for the emerging digiterati, the Internet was described to readers as "[evolving] in its fractious decentralized way through the Internet Engineering Task Force … [In] the cyber '90s … the True Masters of the Universe are not freemasons, mergers-and-acquisitions specialists, or venture capitalists but the members of a voluntary association of tech wizards that create and oversee the technological future of the Internet. It is the IETF's work on tough technical

problems that will make possible the whiz-bang Net applications of the future" (Barsook, 1995) (c.f. Goldsmith & Wu, 2006, p. 23). The IETF's eminence has been further reinforced as scholarly discussions of Internet governance during this period give privileged attention to the IETF and its working methods (Barsook, 1995; Goldsmith & Wu, 2006; Hofmann, 2005; Mueller, 2002). Such attention not only fortified the IETF's position as the "principal body engaged in the development of new Internet Standard specifications," but also made Internet governance synonymous with the IETF. Again, this was not to suggest that the IAB and IESG were inconsequential but rather that their activities supported a structure which was consolidated around the IETF and its working groups. If user control of the standard process prior to POISED had been an aspiration of the global Internet community, in its aftermath it was established as 'fact' through the new IETF and the revised standards process.

'Standard' performances: *rough consensus and running code* as 'Best Common Practice'

Because the controversies that established the IETF as the authority for global Internet governance had to do with the position and power of users, the debate ultimately revolved around the procedures for making Internet standards. The legitimation of the IETF working groups thus went hand-in-hand with a new set of standards procedures, which were stipulated in RFC 1602 (The Internet Standards Process – Revision 2). Defined with the objective of ensuring user-driven participation, these procedures were designed to ensure that the IETF governance system protected and promoted 'open access.' This was formally expressed as the Internet Standards Process expanded from its focus on standardizing technical protocols

to include the actual practices by which those protocols were made. In this way, the procedures outlined in the RFC 1602, and in subsequent standards decisions, were established as governance practices.

The reaction to the IAB memo demonstrated that any technical proposal, even if it was a workable solution, would have difficulty being accepted as an Internet Standard if the process by which it became a standard was viewed with suspicion. Standardizing technical requirements was therefore also a matter of standardizing the methods and procedures by which the Internet architecture evolved. Doing so was not a matter of putting process before technical competence. Echoing their earlier criticism of the ISO, IETF participants argued that without the deliberative, grassroots, and participatory approach, technical standards would lack competence and the confidence of the users. Without consensus no specification would have a "realistic chance of commanding compliance" (Hofmann, 2005, p. 9). Accordingly, in the course of moving authority from the IAB to IETF working groups, a new set of operational procedures were adopted that would enhance openness and put decision-making power in the hands of the 'Internet community.' Russell (2006, p. 31) therefore argues that the 1992 crisis must be understood for how it "forced engineers in the IETF and the IAB to examine their core *procedural* beliefs" (my emphasis).

RFC 1602 listed the three goals of " (1)…creating specifications of high technical quality; (2) the need to consider the interests of all of the affected parties; (3) the importance of establishing widespread community consensus" as the key requirements for developing Internet standards (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 6). By defining the IETF as the principal site for standards-making, the brunt of its work occurred in its different working groups (c.f. Bradner, 1996; Bradner, 1998). To encourage

widespread participation within the 'Internet community' — understood as "the entire set of persons, whether individuals or entities, including but not limited to technology developers, service vendors, and researchers, who use the Internet directly or indirectly, and users of any other networks which implement and use Internet Standards' (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 27), — working group activities had to take place in a "public forum" "[conducting] much of its business via electronic mail distribution" (Bradner, 1998, p. 11). Using mailing lists was not meant for making use of a new technology, but to overcome the difficulties of travelling long distances to meet 'face-to-face,' that for many users could be a barrier to participation. From time to time working groups might have to meet outside of the list to "discuss and review tasks, to resolve specific issues and to direct future activities" (Bradner, 1998, p. 11). However, discussions in face-to-face meetings were always subsidiary to discussions on 'the list.' The working group guidelines stipulated that any "decisions reached during face-to-face meetings … MUST be reviewed by the mailing list" (Bradner, 1998, p. 12). Once a working group came to a 'rough consensus' regarding a technical specification, it was put to the IESG, which in turn formed a committee to review the standard and "provide an objective basis for agreement with the Internet community that the specification is ready for advancement" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 19). Shortly thereafter the IESG would "communicate its finding to the IETF to permit a final review by the general Internet community" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 19).[44] Also, although participation was open to anyone who wanted to join, no one was

[44] IETF participants were not naïve about the problems of open communication, particularly as users with different levels of expertise and experience attempted to collaborate: "Proposed working groups often comprise technically competent participants who are not familiar with the history of Internet architecture or IETF processes. This can, unfortunately, lead to good working group consensus about a bad design" (Bradner, 1998,

permitted to represent other entities. Instead, participation occurred through "individual technical contributors, rather than by formal representatives of organizations" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 8). On the one hand, individual participation can be seen as a direct product of the user-empowerment and open architecture principles embedded in the Internet's technical design. On the other, one can surmise that, based on previous experience, this was a way to obviate the influence of governments and corporate entities. Unlike the ISO and the ITU, the IETF was decidedly not an inter-governmental organization (Hofmann, 2005, p. 9).

Altogether, these specifications were intended to "provide ample opportunity for participation and comment by all interested parties" and provide mechanisms that facilitated repeated discussion and debate in open platforms "at each stage of the standardization process" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 4).

Read as a whole, the emphasis on working group deliberations via worldwide mailing lists reflected the principle of 'open access' not only by trying to include as many members of the 'Internet community' as possible. By further specifying that agreement had to be reached by 'rough consensus' and that the final review of standards was always undertaken by the wider IETF community (rather than just the working group) to guide the decision of the IESG, the new standards process put standards authority in the deliberated opinion of a wider community of users.

The prescriptive nature of these procedures – that is, their definition as Internet governance *routines* – was made explicit when the Internet Standards Process was adopted.

---

p. 8). To this end, IETF Working Group Guidelines allowed that "an Area Director may assign a Consultant from among the ranks of senior IETF participants" to help facilitate more effective discussion within working groups (Bradner, 1998, p. 8).

In light of events that precipitated the POISED Working Group, RFC 1602 issued the following recommendation for future standards development:

> Although Internet standards have generally been concerned with the technical specifications for hardware and software required for computer communication across interconnected networks … good user service requires that the operators and administrators follow common guidelines for policies and operations. While these guidelines are generally different in scope and style from protocol standards, their establishment needs a similar process for consensus building. Specific rules for establishing policy recommendations and operational guidelines for the Internet in an open and fair fashion should be developed, published and adopted by the Internet community. (Internet Architecture Board & Internet Engineering Steering Group, 1994: Appendix C)

Following their own recommendation, in the subsequent iteration of the standards-making guidelines –RFC 2026 – "The Internet Standards Process – Revision 3" (Bradner, 1996) – IETF users agreed to introduce a new kind of Internet standard: "Best Common Practice." Best common practices were intended "to standardize the practices … of community deliberations" and provide a "vehicle by which the IETF community can define and ratify the community's best current thinking on a statement of principle or on what is believed to be the best way to perform some operations or IETF process functions" (Bradner, 1996, p. 15). The publication of RFC 2026 itself as a 'best common practice' was not just a document to describe standards-making procedures. For robust and widely accepted technical standards to be created, these were the required practices. With the prescriptive force of a standard, the Internet Standards Process would ensure that standards making would meet the requirements of both technical superiority and participatory integrity. 'Internet protocol' was both the product and the specification of a *legitimated* decision-making process.

To the degree that 'best common practices' were intended to "… define and ratify … a statement of principle" (Bradner, 1996, p. 15) they demonstrated that the procedures for standards making had a profound normative significance. Stipulating open participation and consensus, 'best common practices' facilitated the production of technical requirements for

the evolving Internet and also ensured that technical development occurred according to the principle of 'open access.' Consequently, by prescribing open, deliberative, public, global, user-driven decision-making, their regular deployment constructed an open, deliberative, public, global, user-driven political order for the Internet. Through the *standardization* of the Internet Standard Process, 'open access' was continually advocated as both the normative goal and the experienced reality of global Internet governance – the prescriptive nature of the Internet Standards Process established routines (repeated practices) that reproduced an Internet political order structured around the IETF's deliberative, user-driven decision-making. In so doing, they made 'open access' both the goal and the expected outcome, which kept the IETF at the front and centre – the needed agency – for the 'acceptable' production of Internet standards.

As 'rough consensus and running code' was both the objective of these routines and the logic of their operation, it constituted the performative logic of the Internet Standards Process. Based on this principle, the Internet Standards Process not only guaranteed that technical standards were devised by user testing and implementation, they also embedded open discussion and deliberated consensus as how standards obtained user compliance. Russell (2006, p. 56) aptly claims that the 'rough consensus and running code' credo articulated a "political philosophy, a style of network architecture and of engineering." Employing and deploying it as the fundamental tenet *and* favoured technique of standards made evident the normative tenor with which the Internet Standards Process operated.

Overall, the Internet Standard Process installed a requisite set of practices and procedures for the creation of technical standards. But more than a set of functional requirements, they imbued the standards-making process with a particular normative agenda.

With ‘open access’ inscribed as the ‘why’ of governance, technical standards as the ‘what’, users in the Internet community as the ‘who’, ‘rough consensus and running code’ as the ‘how’ and IETF working groups and their mailing lists as the ‘where’, the *global village* appears to have ceased to be a metaphor. Through the IETF’s user-driven, bottom-up standards-making process, its influence on the academic community had contributed to literal definition of global Internet governance. Moreover, following the Internet Standards Process meant that ‘open access’ was constantly performed in a set of practices. This not only kept the metaphor’s legitimating power alive, it sanctioned the IETF’s central position in the governance system – without the IETF’s Standards Process, standards might not meet the test of user testing and rough consensus. If explicit reference to the *global village* no longer circulated in the language around Internet governance, it would be hard to deny the metaphor’s influence on the ways in which it was conducted.

Restricting ‘restricted access’: ‘open access’ and the closure of sovereignty

Inscription is an asymmetrical process. The legitimation of one perspective as the ‘facts’ excludes or subordinates the validity of other perspectives. This delegitimation does not necessarily remove other perspectives from political discourse at large, but it does put them in a subordinate position. The influence of the *global village* metaphor and its consequences for the globalization of the Internet systematically foreclosed the *state of nature* metaphor and the legitimacy of sovereignty as a frame of reference for networking research and management.

Sovereignty's subordination was evident initially as the shift from security to education moved networking authority from the NSF to the DCA. If the NSF, as a government agency, still represented sovereign influence, despite it efforts to promote a more universal Internet, the privatization of the NSF backbone removed its involvement in Internet governance. Controversies around sovereignty heated up in the IETF's break with the ISO, though its last vestiges were removed in the restructuring of the IAB-IETF relationship, the revision of the Internet Standards Process, and its adoption as an 'Internet standard.' If Internet governance had been defined and legitimated through the terminologies of *national defence*, *security,* and *territoriality*, the inscription of the *global village* metaphor provided more than an alternative. It also dislodged their powerful hold over the political imagination. Although the metaphor operated remotely, it influenced the definition of the Internet as a worldwide communications medium that was user oriented and governed through consensus. In brief, sovereignty's nexus between *territory*, *population*, *authority,* and *recognition*, which had created the Internet as a national security project, was dismantled by a normative vocabulary of deterritorialization in which *territorial* restrictions were removed by using TCP/IP to build worldwide communications networks, *populations* were defined according a community of users, *authority* was placed in deliberative working groups, and *recognition* was established through 'rough consensus.'

Ironically, the vocabulary of 'open access' itself generated exclusions. Although email, newsgroups, and virtual communities were proliferating, the Internet of the 1980s and early to mid-1990s remained largely a research medium or platform of technical experimentation. Popular applications such as the World Wide Web had yet to transform the Internet from its research origins to a mass communications medium. Consequently, although

the focus on 'users' was intended to imply a more universal community, users usually had the requisite technical expertise to use the Internet. Even the IETF, which defined itself as an organization with open membership, where "participation is open to all" and "anyone from the Internet community who has the time and interest to participate [was urged] to participate" (Bradner, 1998, p. 3), stressed that users had to have a certain level of technical proficiency and knowledge. The global 'Internet community' was also limited to users who "implement and use Internet Standards" (Internet Architecture Board & Internet Engineering Steering Group, 1994, p. 26). They tended to be white, middle-aged, university-educated men (J. Katz, 1997) (c.f. Wellman & Haythornthwaite, 2002).[45] For this reason, initiatives to bridge the 'digital divide' have not simply focused on providing underprivileged groups (usually in the developing world) access to computers and other Internet technologies. They have also put a priority on increasing the involvement of underrepresented groups in the technological discussions about the Internet's evolving architecture (United Nations, 2003: Article 10).

Alternative explanations: *global village* by (technological) design

The plausibility of this account of the *global village* metaphor and its relationship to the Internet and its governance relies on its ability to overcome the weaknesses in contending approaches. As argued, in many accounts, the Internet's open and distributed architecture and it end-user empowerment principle is said to naturally give way to a *global village*

[45] Barsook (1995) notes that women made up about 10% of the IETF participants, which was proportionate the percentage of women who used the Internet at the time.

(Rheingold, 1994).[46] Advocates of this view, mostly cyberlibertarians, suggest that because the Internet's networks, its users, and the information sent over the Internet cannot be located or contained within a particular state's territory, the Internet necessarily compromises the authority of sovereign governments and generates grassroots participatory governance frameworks. Regardless of whether social forces had tried to maintain the Internet as a technology of national defence, the Internet's technical architecture has its own momentum and would have generated a *global village* polity (Barlow, 1996; Negroponte, 1995).

Certainly there is something to be said about the Internet's unique design principles. However, technology never evolves in a vacuum (Bijker, Hughes, & Pinch, 1987; Misa, 2004). Internet 'code,' as Lessig (1999) has made clear, can be designed to reflect certain values and enable specific kinds of politics. This is not to shift the focus completely to 'ideational' factors and ignore the hard-reality of Internet cables, routers, etc. Certainly, the Internet's technical design lends itself to globalizing potentials. Without the development of TCP/IP, for instance, inter-networking on a global scale would not have been possible. However, as the discussion in this chapter has tried to show, the Internet's architecture can be deployed toward different ends – sovereign and global. Specifically, the argument is that the Internet's association with a *global village* was not the simple outcome of its "revolutionary" technological characteristics. Rather, putting the focus on metaphors, I have tried to how that technology was situated within an evolving normative context. The *global village* operated as

[46] TCP/IP and DNS constitute the Internet's basic design as a distributed and decentralized system of information transfer. Transmission Control and Internet Protocol (TCP/IP) constitutes the distributed structure that allows data transfer between all computers on the network in a non-hierarchical fashion. Each computer on the network is identified by an Internet Protocol address (a series of numbers such as 1234.5678.4321) that allows data to know where it is going. TCP ensures that data gets where it wants to go. The Domain Name System relies on a hierarchical but decentralized system of information transfer. End user empowerment is often defined as the *'end to end'* principle. As the network is dumb to the kind of information transported (for instance, movies, email message, photos), the network's complex functions are left to the end-points, where users require the applications to use the information. Applications are thus developed and added at the end-points according to the needs and desires of different users.

a metaphor of globalization and came to influence the evolution of the Internet's technological design and management as a global, non-sovereign, participatory medium.

As the significance of metaphors rests in their legitimating power, the articulation of the *global village* metaphor in the context of the 1960s American counter-cultural movement and its association with computing validated a vision that linked the computers and computer networks to the aspiration of creating a more harmonious, peaceful and deliberative world order. Indeed, the appropriation of McLuhan's metaphor did not become the explicit credo of the computer science community, but it did influence certain members involved in the ARPANET. More significantly, though, the suggestion of the metaphor converged and overlapped with existing approaches in the academic community's approach to networking research. Having a mutually reinforcing effect, they undermined and destabilized the 'restricted access' protocols of defence cultures with new ideas about opening access to networking by expanding membership, open discussion, consensus and grassroots decision-making. This ethos was strengthened as the ARPANET went 'rogue' (that is, defence contractors did not always maintain the security protocols that military minds preferred) and became a civilian network. Demands by other civilian researchers to have the opportunity to engage in similar networking experiments were therefore inevitable. The force and significance of the metaphor amidst these developments can be pinpointed in the way it endowed computing with a specific normative potential, and in particular, one that was linked to a global project, not a national one. The technology, therefore, evolved *within* the normative nexus of the *global village* metaphor, the academic approach to networking research and greater demands that networking be 'opened' up the public. In short, although

TCP/IP, amongst other design features, made possible a global Internet, it did not in and of itself make the Internet a *global village*.

More explicitly, the role of the metaphor in affecting changes that allowed the Internet to evolve as a *global village* had to do with the consolidation of a particular vocabulary. No longer was TCP/IP a way to fortify borders by enhancing defence communications; instead, it was a way to transcend them and foster public and global communication. The NSF's *Acceptable Use Policy* was one vehicle of this consolidation. It also explicitly demonstrates that the Internet's deployment as an educational, public and global communications medium had to do with political changes – specifically the transfer of authority from defence agencies to the NSF – rather than the inevitable outcome of a communications system structured as decentralized networks. In fact, it was only after the NSF opened up the NSFNET backbone to 'foreign' connections that the Internet's evolution as truly planetary network of networks became possible.

Another vehicle for the metaphor, of course, was the technical community. Largely influenced by the NWG's initial practices of user-oriented development, it furthered the inscription of the *global village* metaphor by contesting sovereign influence through user-driven standards development. In conjunction with the notion that the Internet could be used for global communication, their efforts to consolidate technical standards in ISOC and the IETF, established a vocabulary that reinforced the definition of standards-making as open, non-proprietary, grassroots, and deliberative – and now on a global scale. The IETF's own internal struggle between its working groups and the IAB, and the eventual revision of the 'Internet Standards Process' further entrenched this vocabulary in and as the practice of Internet governance.

In sum, the 'global' governance of the Internet described in this chapter was indeed a product of certain features of technological design (decentralized and distributed networking). But, just as importantly, it was also a product of how these were captured and developed by a political ethos that promoted global civilian communications and in turn open, deliberative practices. There may have been a 'fit' between the decentralized network design and the NWG's philosophy and IETF's approach to standards (c.f. Deibert, 1997b; Deibert, 2003; see also Turner, 2006). But this only demonstrates that there is a complex interplay of the 'brute' physical design of the Internet and the normative context in which it evolves. To make the point differently, the Internet evolved globally not only because of its physical-reach across the planet but the way this reach was enabled and shaped by a specific vocabulary – the *village* – which promoted deterritorialized communications. Accordingly, to the degree that the IETF was the institutionalized embodiment of the Internet's 'radical' politics, it was not because the Internet's basic architecture naturally gives way to certain kind of politics. Instead, it was because of the political principle – 'open access' – that defined the Internet's use and its governance practices.

This is not to caution against the use of the *global village* metaphor in discussions of the Internet, its political potential, and its global governance – far from it. Popular culture demonstrates the degree to which the two are difficult to separate. The question is not whether the metaphor should be used to describe the Internet; the question is how and why *global village* became inscribed into the technical and popular imagination about what the Internet is and what it should be used for (c.f. Turner, 2006).

Conclusion

In this chapter I have investigated how the *global village* emerged as a discursive context for political order and how it then came to have an influence on Internet governance objectives, institutions and practices. I have contended that the Internet emerged precisely at a time when promoting cross-boundary communications was considered essential for preventing the outbreak of another devastating war. Its planetary communicative capacities thus immediately found resonance with political activists. However, how this came to inform Internet governance entailed a less obvious set of developments. I have attempted to show that the influence of the metaphor would likely not have been possible had it not converged with a group of young academics that were given the responsibility to develop the technical protocols that would allow inter-networked communications. This is not to say that that the metaphor did not inform their deliberations and approach to computing research. I have demonstrated that even though the *global village* metaphor operated at a distance, it played a part in influencing the academic notion of 'open access' that in time became the legitimating principle for developing and governing the Internet as a global technology (Barbrook, 2008; Turner, 2006). The inscription of the *global village* metaphor in Internet governance debates therefore not only depended on social and political conditions in which it became an 'attractive way to speak about the world,' it became possible because it converged with the particular interests and commitments of the young graduate students, who even if they did not overtly refer to the metaphor, became vehicles for its dissemination.

Putting the focus on how 'open access' proposed a new terminology in which the evolving Internet was defined as a *civilian*, *non-commercial*, *accessible*, *voluntary*, *non-proprietary*, *people-to-people communications* medium that promoted *user-empowerment*, I

have examined how the *state of nature* metaphor's principle of 'restricted access' and its vocabulary of *territoriality*, *security* and *defence* were displaced. I have attempted to show that this resulted in the normative deterritorialization of the Internet – that is, its globalization – by removing *territorial* borders as a restriction on inter-networked communication, expanding *population* to include a worldwide community of users, placing *authority* in a decentralized, bottom-up working groups, and making consensus the basis of *recognition*. Basically, 'open access' removed sovereignty – both in terms of its security impulses and also through the role of governments – as a legitimating principle for Internet governance.

Examining how users were able to galvanize around 'open access,' I have described how governance efforts became consolidated around the IETF's working groups. In turn, I have demonstrated that because 'open access' informed the procedures that developed Internet standards, the Internet Standards Process became governance practices. Based on a performative logic of 'rough consensus and running code,' I have argued that the routine observance of the Internet Standards Process not only helped to construct a global political space as public, communicative and user-driven but that because of its deliberative approach to standards development, the Internet Standards Process reproduced it. In other words, if governance is about the production and performance of 'facts' that constitute a political order, in this chapter I have examined how the influence of the *global village* metaphor on networking research constituted a global Internet order by instituting 'open access' as the 'why' of Internet governance, Internet standards as the 'what,' a worldwide user community as the 'who,' IETF working groups as the 'where' and the 'rough consensus and running code' as the 'how'.

Chapter 2

Global Marketplace: 'Competition' and ICANN

A different metaphor that I think comes closer to describing a lot of the activities that will take place [on the Internet] is that of the ultimate market … It will be where were we social animals will sell, trade, invest, haggle, pick up stuff …
~ Bill Gates

Introduction

Bob Maher, outside counsel for McDonald's Corporation, happened to be reading *Wired* when McDonald's called asking if he knew of the magazine. Wired reporter Joshua Quittner (1994) had written an article about the registration of the "mcdonalds.com" domain name, or web address. Quittner recalled how he had contacted McDonald's media relations department to inquire if the company intended to have an Internet web address and asked if he could register 'mcdonalds.com.' The representative asked: "Are you finding that the Internet is a big thing?" With no outright objections, Quittner registered the name. He asked his readers how much the domain name was worth and whether he should consider auctioning it off to, say, Burger King or Wendy's.

It was 1994. The World Wide Web, introduced only two years earlier, was stimulating a new phase of unprecedented Internet growth. The 'mcdonalds.com' incident, however, suggested that something new was afoot. Domain names, intended as mnemonic devices for long Internet Protocol (IP) addresses, were the Internet's new real estate. The right domain name could potentially reach consumers all over the world. Quittner's article

drew attention to entrepreneurial individuals who were registering famous domain names in the hopes that they could make a profit by selling them back to corporations. Quittner's article therefore implicitly demonstrated that the new popularity of the Internet was not simply about its communicative powers but also its commercial potential.

The rush for domain names was emblematic of new efforts to promote the Internet's globalization during the mid- to late- 1990s. The end of the Cold War had reduced the fear of nuclear annihilation and a possible Third World War. The subsequent fall of the Soviet Union reinforced the primacy of global capitalism. Consequently, the 'new world order' would be defined by the power of the global economy rather than great power competition. Neoliberal economic policies became the norm as governments around the world advocated faith in the 'self-regulating' logics of the market and deregulated their national economic sectors to increase their competitiveness in the 'global marketplace.'

Whether opportune or accidental, this geopolitical and economic shift coincided with the growing popularity of the Internet. Because territorial borders did not circumscribe its technical architecture, the Internet appeared to give literal expression to the *global marketplace*. Governments, corporations, and the popular press all agreed that "[with] the Internet, the whole globe is one marketplace" (Flichy, 2007, p. 186). Thus, the *global marketplace* metaphor emerged not only as a way to represent the globalizing economy. To the extent that the Internet facilitated economic globalization, it also represented the Internet's global potential.

In this chapter, I describe how the popularization of the Internet as a *global marketplace* generated distinctive patterns and practices of global Internet governance. While numerous governance issues were associated with the metaphor – digital copyright debates,

the introduction and regulation of proprietary software, and the Internet advertising, amongst others – I focus on the rush for domain names. As having a presence on the Internet requires a domain name, commercial Internet use raised questions about who was entitled to a specific web address and whether domain names themselves could be competitively bought and sold. These questions drew attention to the role of sovereignty in Internet governance. Because the National Science Foundation (NSF) managed the domain name space (DNS), the US government was criticized for creating a monopoly. Efforts to remove sovereign influence converged around the need for 'competition' and 'privatization' and resulted in the creation of a new private corporation – the Internet Corporation for Assigned Names and Numbers (ICANN), which relegated governments to an advisory position, implemented a global body of trademark laws, and limited the participation of individual users. In striving to create a competitive global market in the domain space, ICANN was a microcosm of the new governance institutions and practices enabled by the *global marketplace* metaphor.

Because governments, especially the United States, played an instrumental role in the creation of ICANN, some observers argue that ICANN is represents the consolidation of sovereign power over the Internet rather than 'deterritorialized' global governance (c.f. Drezner, 2004; Goldsmith & Wu, 2006, pp. 167-188; Mathiason, 2007; Mueller, 2002). Yet, as my discussion will show, governments, spearheaded by US efforts, did attempt to extricate themselves from Internet governance. Specifically, I will argue that the US government's advocacy of the *global marketplace* in Internet global governance played a part in implementing a new discourse of globalization and, in turn, a new set of legitimating principles that devalued the participation of governments on the basis of sovereignty. Thus, even with the prominent role of the US government, the discursive context of the *global*

marketplace provided a new vocabulary of deterritorialization and promoted new institutions and practices of global governance.

Controversies about ICANN persist today, in part because ICANN's full privatization is still contingent on meeting certain requirements and conditions imposed by the US Department of Commerce. While these recent developments are important in understanding ICANN's (and the US government) part in global Internet governance today, they are not the focus of this chapter. It considers only the conditions that entrenched the *global marketplace* metaphor in popular discussions about the Internet such that ICANN became the 'logical' institutional response. My discussion therefore ends in 2000, two years after ICANN's incorporation and the year initially intended for its release from US oversight.

This chapter draws heavily from Milton Mueller's (2002) *Ruling the Root*, perhaps the seminal study of ICANN's formation. With its extensive recording of different stakeholders' policy positions and interviews with key actors, it is a primary text for understanding the discursive milieu surrounding ICANN's formation. Yet drawing from institutional economics and regime theory, Mueller presents ICANN as an inevitable outcome of property right conflicts in the domain names space. As a counter-point, I re-read Mueller's analysis through the tools of genealogy and critical discourse analysis and supplement his account with other primary documents, demonstrating that the dynamics he explains can only be fully accounted for by considering the normative influence and legitimating power of the *global marketplace* metaphor.

Globalization, the *global marketplace,* and the Internet

The neoliberal economic reforms undertaken by Western-industrialized countries in the 1980s disseminated the *global marketplace* as a metaphor of globalization. According to Sparke (2006, p. 157), "while neoliberalism certainly represents a revival of classical nineteenth century free market liberalism, it is also clearly a new kind of capitalist liberalization that is distinct in so far as it has been imagined and implemented *after* and *in opposition to* the state-regulated national economies of the twentieth century." Economic governance was restructured to promote greater privatization and foster competition. Privatization was not limited to the economic realm; rather the market was seen as the appropriate basis for governing all parts of society (Castells, 2000b, p. 137; Fairclough, 2001, p. 127; Harvey, 2005a, pp. 160-165).[47]

Deregulation, liberalization, and privatization were not simply policies for domestic governance – promoting competition was the basis for building a new kind of *global* economy. The global market was portrayed as driven by a set of inevitable and irreversible logics (Barney, 2004; Beck, 2005; Steger, 2005). There was, as Prime Minister Thatcher said, 'no alternative' but to embrace it. The fall of the Soviet Union furthered this view of global market forces as 'inescapable.' According Fukuyama (1992), the failure of Soviet-led communism was the 'end of history' because it demonstrated that capitalism was the only legitimate model for viable economic and political societies.

Facing 'no alternatives,' and likely because the prospects of a nuclear war or some kind of violent confrontation between great powers had been diminished, Steger (2005, p. 33) argues that " 'the self-regulating' market [became] the normative basis for … global order" (c.f. G. H. W. Bush, 1990; Fukuyama, 1992). Globalization emerged in a new guise – the

[47] Fairclough (2001: 127) described the neoliberal agenda as marked by a "restructuring of relations between economic and non-economic fields which involves an extensive colonization of latter by the former."

capitalist *global marketplace*. According to Barney (2004, p. 72), defined in the context of the *global marketplace* metaphor, globalization "… names not only the organization of the capitalist economy across national political borders, but also the constitution of that economy on a neoliberal model – in which market actors are increasingly free of regulatory constraint and states find their interventionist and redistributive options increasingly hedged – whose adoption has reached near-universal levels."

Based on this construction of globalization, the *global marketplace* renders a normative challenge to the *state of nature* metaphor. Despite an emphasis on violent and competitive political logics, Hobbes' defence of the sovereign state implies that sovereigns in part create the conditions of individual security by providing individuals with social and economic welfare. Endowed with the responsibility of ensuring security from the 'outside,' sovereigns must also "uphold … the Industry of their Subjects," to allow them to obtain a "commodious living" (Hobbes, 1996, p. 90). State leaders not only protect their citizens from external violence, they also shelter them from external forces that may impinge on the autonomy of national communities to determine for themselves the conditions of their socio-economic well-being. Sovereignty therefore legitimates the state apparatus for military security and defines the state as the appropriate institution for providing socio-economic welfare (Castells, 2000a: 386; , 2004: 363-5; Murphy, 1996).

Under the descriptive force of the global self-regulating market, sovereignty became problematic for economic growth. Not only were states considered functionally incapable of autonomously managing the economy in the face of *global* market forces, sovereignty was considered to be a detriment to prosperity. Now competing for "[global] market share rather than for territory," giving up state authority was a "condition of admission" to the global

economy (Barney, 2004, p. 22). As neoliberalism became policy orthodoxy, states surrendered their authority to self-regulating 'private' agencies, whose legitimacy was based on their ability to foster a competitive global market (Porter, 2005). Deferring authority to the global market, global governance was understood as a system in which "private sector markets, market actors, non-governmental organizations, multinational actors and other institutions exercise forms of legitimate authority" (Hall & Biersteker, 2002a, p. 4) (c.f. Cutler, 2002; Cutler, Haufler, & Porter, 1999).

Although many saw this shift as the 'end of the state' (Ohmae, 1995; Strange, 1996), states continued to be important political agents, supporting the creation of regulatory environments that facilitated global competition and the integration of national economies into the global market. Although national regulation was intended to be minimal, specific legal and regulatory frameworks were needed to facilitate competition (Beck, 2005, p. 85; Harvey, 2005a), as demonstrated by efforts to redefine domestic policies regarding economic growth and in the creation of global regulatory frameworks and institutions, such as the World Trade Organization. As Fairclough (2001, p. 130) asserts, the global marketplace transforms states into 'nodes' in the global economy and creates a new corporate-business-state governance complex "focused on creating the conditions (the financial, fiscal, and legal structures, the 'human capital' and so on) for successful competition in the new global economy" (c.f. Castells, 2000b; Harmes, 2006). Weiss (1998) argues that state facilitation of global market forces is evidence of continued state sovereignty, despite the pressures of economic globalization. In fact, she defines economic globalization as a state-directed project. However, other commentators have shown how states' deregulatory efforts have actually ushered in new regulatory measures that gave greater 'sovereignty' to global capital

markets (Hardt & Negri, 2000; Sassen, 2000). Although states have been seminal in constructing the global market (Hall & Biersteker, 2002a, p. 6), in time, the market has exerted its own 'disciplinary' effects (Gill, 1995; Harmes, 2006) (c.f. Sassen, 2006).

The *global marketplace* metaphor's normative deterritorialization of sovereign political order prized the vocabulary of *deregulation*, *denationalization*, *liberalization*, *competition,* and *privatization* against sovereignty's commitment to *the public*, *national economic welfare,* and *protection*. In this new "borderless economy" (Ohmae, 1990), capitalism operated in a "great planetary marketplace" where market share, not *territory*, was the metric of political power (Gates qtd. in Cosgrove, 2001, p. 265). Consequently, *population* no longer designated a body of national citizens but the set of global consumers, *authority* was granted to market mechanisms and their private agents, not public government agencies, and *recognition* amounted to acceptance of a putative global regulatory system in lieu of territorially demarcated and autonomous legal jurisdictions. In short, global competition replaced sovereignty as the basis of political legitimacy.

By the mid- to late- 1990s, the *global marketplace* became the defining motif of globalization. Pundits such as Martin Wolf spoke of globalization as "the great economic event of our era" (Wolf, 2001, p. 9). Participating in the global marketplace became a central goal in international and multilateral fora, such as the World Trade Organization, APEC, the International Monetary Fund, and the World Bank (Held, 2004; O'Brien, Goetz, Scholte, & Williams, 2000; Woods, 2006). Academics also joined the fray, arguing that "markets are effectively deterritorialized, [with] a growing incompatibility between the political boundaries of states and the economic boundaries of markets" (Stephen J. Kobrin, 2002, p. 67). Global market discourse reached its apogee in the aftermath of the 1997 East Asian

financial crisis, whose worldwide effects made the global scope of the market truly evident. Policymakers and academics therefore stressed the need to build a stable '*global* financial architecture' (Blinder, 1999; Eichengreen, 1999; Noble & Ravenhill, 2000; Stiglitz, 1999). The *global marketplace* was not without its critics. However, in targeting neoliberal economic policies, the vocal opposition from the 'anti-globalization' movement implicitly authorized the discursive construction of globalization as a *global marketplace* (Eschle & Maiguashca, 2005; Fisher & Ponniah, 2003; Hardt & Negri, 2000; N. Klein, 2002).

Although not the decisive factor, the Internet figured prominently in discussions about the emergence of the global economy (Bhagwati, 2004; Castells, 2000b). Theories of post-industrialism (Bell, 1973), information society (Webster, 2006), and post-fordism (Amin, 1994) all put a high premium on the transformative effect of new information technologies in restructuring capitalist modes of production. As Castells (2000) described it, information technology, of which the Internet was the seminal example, transformed industrial econom*ies* into a new informational and global econom*y*.[48]

The connection between the new economy and the Internet went beyond its impact on capitalist production. The Internet was considered an economic space of its own. Specifically, situating the Internet within the context the *global marketplace* metaphor generated new enthusiasm for global electronic commerce: US President Clinton's *Framework for Global Electronic Commerce* (*Framework for Global Electronic Commerce*,

[48] Castells (2000b, p. 77) says that this new economy is *informational* as the generation and distribution of knowledge takes on a primary significance and *global* as developments in technology allow for the capacity to work in real time on a planetary scale. Castells acknowledges that capitalism has operated on a worldwide scale. However, what is new is how economic production has taken on a more networked morphology. Thus, the instantaneity of flows, and the ability to manage production in real time marks a shift from a 'world' to a 'global' economy (see also discussion Castells, 2001, pp. 101-102).

1996) explicitly referred to the Internet as "a global marketplace."[49] Both the EU and the Netherlands issued statements that asserted, "[t]he Internet should grow as a seamless, decentralized, global marketplace where competition and consumer choice are the main drivers of economic activity."[50] Agreements were forged to facilitate global electronic commerce in APEC, the EU, the OECD, the G8, the WTO, and the United Nations.[51] To say that the "Internet was *born* as a global marketplace"[52] was common parlance (my emphasis).[53] Promoting its economic potential was therefore a primary objective.

As stated, in this chapter I trace how the popularity of the *global marketplace* metaphor precipitated debates about how to introduce competition into the domain name space and resulted in legitimation of ICANN. Although this is a limited discussion of how global Internet governance was influenced by the *global marketplace* metaphor, the domain name issue proved to be essential in fostering economic activity on the Internet. Thus, a

---

[49] The Clinton Administration's Framework for Global Electronic Commerce. Executive Summary. http://www.technology.gov/digeconomy/11.htm [Accessed: 23 January 2007]. Although electronic commerce is not limited to the Internet, and includes transactions via telephone, fax, and other telecommunications technology, the Internet was the focus of discussions. In almost all documents I have consulted, the Internet was key to successful e-commerce strategies (Margherio, 1998).

[50] Joint Statement on the Development of the Internet and the Promotion of Global Electronic Commerce. October 21, 1997. Washington, DC. http://www.technology.gov/digeconomy/dalwijrs.htm; United States and the European Union Reach Agreement on Global Electronic Commerce.http://www.technology.gov/digeconomy/20.htm (Business America: The Magazine of International Trade, Vol.119, No.1, January 1998) [Accessed: 25 January 2007].

[51] APEC (1998) Blueprint for Electronic Commerce http://www.apec.org/apec/leaders_declarations/1998/apec_blueprint_for.html; European Ministerial Conference on 'Global Information Networks: Realizing the Potential" OECD (1997) Dismantling the Barriers to Electronic Commerce http://web.archive.org/web/20010413165550/http://www.oecd.org/dsti/sti/it/ec/prod/dismantl.htm; G8 (1998) Minister's trade regulations for the Internet;; WTO (1998) Declaration on the Global Electronic Commerce http://www.wto.org/english/thewto_e/minist_e/min98_e/ecom_e.htm; UNCITRAL (1996) Model Law on Electronic Commerce with Guide Enactment www.uncitral.org/english/texts/electcom/m/-ecomm.htm [Accessed 24 January 2007].

[52] Joint Statement on the Development of the Internet and the Promotion of Global Electronic Commerce. October 21, 1997. Washington, DC. http://www.technology.gov/digeconomy/dalwijrs.htm [Accessed: 26 January 2007].

[53] Other e-commerce initiatives: UNCITRAL (1996) Model Law on Electronic Commerce with Guide Enactment www.uncitral.org/english/texts/electcom/m/-ecomm.htm; the G-7's Annual Conferences on "Global Marketplace for SME's"; G8 Minister's trade regulations for the Internet (1998), European Ministerial Conference in 1997 on 'Global Information Networks: Realizing the Potential"; WTO Declaration on the Global Electronic Commerce (1998)

discussion of the events surrounding the formation of ICANN effectively illustrates how the *global marketplace* metaphor globalized the Internet as an economic platform and the consequences this had for global Internet governance.

Legitimacy crisis: disrupting 'public resource management' and 'open access'

Although seeing the Internet as a platform for the *global marketplace* is commonplace, the association between the two is relatively recent. As Flichy (2007, p. 179) argues, for its first twenty or so years, the Internet developed outside of the market economy. Rooted in principles of 'open access,' "market exchange was even proscribed." Formally stated in NSFNET's *Acceptable Use Policy*, the Internet's 'immunity' from market logics was also was taken for granted: community norms implicitly prohibited commercial use of the Internet. This aversion to commercial activity is in part explained by the overwhelming academic influence on the development of the Internet, and that community's general disdain for business (Brand qtd. in Flichy, 2007, p. 192). However, it was also a product of how the *global village* metaphor had informed approaches to computing and network research and management.

In the mid-1990s, a constellation of forces – from within the Internet's governing structures and also the general political climate at the time – interrupted and undermined the assumptions and practices inscribed by 'open access.' Specifically, commercial use of the Internet became an acceptable practice and placed the Internet at the forefront of the growing enthusiasm for the neoliberal *global marketplace*. Although opening the Internet to commercial activities disrupted the influence of the *global village* metaphor on Internet

governance, it directed more attention to how lingering sovereign influence over the Internet hindered commercial competition.

Two main developments enabled the Internet's commercialization. The first was the introduction of the World Wide Web (WWW or 'Web') by Tim Berners-Lee in 1992.[54] Using a hypertext 'browser' (initially Gopher and Mosaic and today Firefox, Internet Explorer, Safari, etc.), the WWW used Universal Resource Locators (URLs), or website addresses, to make it easier locate and access data stored on the Internet. This user-friendly interface popularized the Internet, transforming it into a mass communications medium. That this supported 'open access' appears to go without saying. According to Berners-Lee, by providing a "single, universal accessible … medium for accessing information," the WWW was created with a 'dream' of enhancing "people-to-people communication through shared knowledge … for all groups" (Berners-Lee, 2000, p. 95). He further argued that the "openness of the Web is a powerful attraction. Everyone can not only read what's on the Web but contribute to it, and everybody is in a sense equal" (qtd. by Brody, 1996, p. 40).

Because domain names removed the need to remember numeric IP addresses, the Web built on the Internet's domain name system (DNS) to facilitate the search for documents and information. For instance, instead of having to remember 1234.5678.1234.5678 to access a document on metaphors of globalization, one could use the URL 'www.globalmetaphors.com.' To find the file associated with this URL, a user's computer would first be directed to a server that held the addresses for top-level domains, in this case '.com' (other examples of top-level domains include: .net, .org, .ca. etc). From there, the

[54] Although the Internet and the Web are used interchangeably, they are in fact two separate technologies. The Web is a user application that is 'added to' or 'layered on' the Internet's basic TCP/IP protocol.

computer would be directed to a server where the 'globalmetaphors' (a second-level domain name) address was hosted.

URLs, however, had the unintended consequence of transforming domain names from mnemonic devices into ways to search for content. Novice users often simply typed in the topics they wanted to learn more about rather than using URLs. As browsers were not yet search engines, failing to provide a proper URL produced an error message. To ameliorate this, browsers were reprogrammed to make .com the default top-level domain. A query for 'chocolate' was consequently directed to 'www.chocolate.com.' In this way, domain names became signifiers with semantic meaning (Mueller, 2002, p. 109), with .com – the top-level domain designated for commercial entities – the easiest to access.

The Web made the Internet easier to use and thus contributed to its growth as a communications medium. However, shortly after the Web's release, the National Science Foundation privatized the NSFNET backbone, making commercial Internet use without contributions to education acceptable (Abbate, 1999, p. 119). As a consequence, URLs effectively became locators of consumer goods and services. For example, a visit to 'www.chocolate.com' might yield a page about chocolate's history in Western culture or it might equally be a site selling chocolate. In a word, the combined effect of the Web's release and the privatization of the NSFNET meant that URLs could be used to advertise and sell consumer goods.

The impact of this commercial activity might not have been so dramatic had the Web's release and the NSFNET's privatization not occurred in the immediate aftermath of the Cold War and the ensuing importance accorded to fostering global capitalism. In this context, once the Internet was opened to commercial activity, the Internet headed

government and business efforts to build a *global marketplace*. This had a transformative effect on how the Internet itself was perceived. The Internet was not simply a tool to build the global market – the Internet embodied the global marketplace. Philip Elmer-DeWitt (1995), Time Magazine's prominent 'cyber-reporter', best captured this sentiment: "Lately a lot of development efforts – and most of the press attention – have shifted from the rough and tumble of … newsgroups to the more consumer-oriented 'home pages' of the World Wide Web … The Net … is turning into a shopping mall." Science and technology scholar Langdon Winner (1997) noted, with regret, that the Internet had become a "new sphere of economic transactions, the sphere of Internet commerce. In effect, a vast cybermall has recently moved into the neighborhood of every village, town and city on the planet, selling … products to millions of potential customers." Bill Gates, Microsoft CEO, argued that the "metaphor … [that] comes closer to describing a lot of the activities that will take place [on the Internet] is that of the ultimate market … It will be where we social animals will, sell, trade, invest, haggle and pick up stuff" (Gates qtd. in Mosco, 2004, p. 51).

In this new 'shopping mall,' having the right web address meant that businesses could use the Internet to reach consumers not just locally but globally. This endowed the domain name components of URLs with significant commercial and economic value. There was consequently a rush to register second-level domain names in the .com space, both because it was dedicated to commercial entities and also because it was the default setting for Web browsers.[55,56] Based on the non-proprietary definition of the Internet as public

[55] Although .com was initially intended for commercial entities, in the mid-1990s, coinciding with the Internet's commercialization, the .com registry was opened to any commercial or non-commercial entity that wished to register a name in that space. Unsurprisingly, because of its familiarity to users, it was and has remained the most popular gTLD.

[56] In 1999, a study entitled "A rose.com by any other name," demonstrated that many companies that changed their names to include .com, .net or 'Internet' – regardless of whether their business had changed or if they even did Internet-related work – experienced an increase in values of their stocks (cited in Mosco, 2004).

communications resource, domain names were initially designed as a common-pool resource to which everyone had equal rights (Mueller, 2002, pp. 57-58). Accordingly, the conventional practice of assigning domain names was on a first-come, first-served basis. In light of the Internet's commercialization, entrepreneurial individuals began registering any available famous names, hoping to sell them back to corporations for a profit or to use them for defamation (Maher, 2006; Mueller, 2002; Quittner, 1996; Richardson, 1996; Ugelow, 1994). As website speculation, squatting, and defamation became rampant, owners of famous names raised concerns about the first-come, first-served practice. They demanded trademark protection in the domain name space not only to safeguard against defamation but also to ensure the competitiveness of commercial activity on the Internet (Dueker, 1996). 'Open access' had sanctioned against proprietary and commercial interests, but once the Internet showed commercial and economic potential, the fight for market share and visibility triggered a struggle over who could claim exclusive rights over a given domain name.

The growing commercial importance of domain names also raised questions about who could distribute domain names. Although the debate with the ISO and the privatization of the NSFNET had effectively removed governments from the business of technical standards-making, the root zone file[57] and the domain name system still remained under US government control. In the formative stages of the Internet, management and allocation of domain names had been contracted out by APRA to members of the Internet user community, specifically the Internet Assigned Name and Number Authority (IANA) run by Jon Postel, a former NWG member and a prominent IETF participant, who was based at the

[57] The 'root' refers to the 'root zone file', a master file – *host.txt* – in which all domain names and their corresponding IP are recorded. This means that although the Internet is a distributed and decentralized system, the root provides a point of central control. It is, as Mueller (2002, p. 6) describes, "the beginning point in a long chain of contracts and cooperation governing how Internet service providers and end users acquire and utilize addresses and names that make it possible for data packets to find their destinations."

University of Southern California. As civilian use of the Internet increased, US defence agencies asked the NSF to financially support and perform the actual registration of names on the civilian Internet.[58] To do this, the NSF signed a limited-term Cooperative Agreement with a private firm, Network Solutions Incorporated (NSI).[59] While IANA maintained responsibility for policies regarding the technical evolution of the domain name and the IP address space, NSI did the actual work of handling requests and inserting them into the Internet 'root' so that all domain names and their corresponding IP addresses could be distributed to the Internet at large.

Viewing the Internet as a public resource, the NSF assumed the costs for registering Internet domain names. However, as the demand for registrations in the .com space surged, the number of requests overwhelmed NSI staff (Mueller, 2002, p. 110).[60] A mid-term consultative review of the domain name registration system recommended that the NSF "begin charging for .COM domain name registrations, and later … for name registrations in all domains."[61] The NSF implemented the recommendation by amending the conditions of the NSI contract, permitting the "imposition of user fees" for .com, .net and .org registrations.[62,63] Charging fees could be considered a transgression of the 'open access'

[58] In particular, the passing of the High Performance Computing Act in 1991 by the US government to support the creation of a National Research in Education Network (NREN) dedicated new resources to promote the growth and development of the civilian Internet.
[59] NSF Cooperative Agreement, No. NCR-9218742. "Network Information Services Manager(s) for NSFNET and the NREN: INTERNIC Registration Services.
[60] In 1994, NSI registered 12, 687 names in the .com space. By February 1996, this number had increased to 232, 004 (Mueller, 2002, p. 110; see Table 6.1 on the same page).
[61] InterNIC Midterm Evaluation Recommendations: A Panel Report to the National Science Foundation (qtd. in Mueller, 2002, p. 282).
[62] NSF Cooperative Agreement No. NCR-9218742, Amendment 4. Proposal No. NCR-9544193.The NSF made the decision to allow fees after holding a consultative review of the domain name registration services. It is worth noting that charging a user fee was not prohibited from the outset. According to the terms of the original cooperative agreement, "the imposition of a user based fee structure" was listed as a possible future change to the contract. (NSF Cooperative Agreement, No. NCR-9218742. "Network Information Services Manager(s) for NSFNET and the NREN: INTERNIC Registration Services.)

principle – after all, an 'open' Internet should be 'freely' available. However, it received little criticism. Users were more concerned that the decision had been made without consulting the user community. As one user put it, "no one has really objected to paying reasonable fees for registration. EVERYONE (almost) had objected to paying fees set arbitrarily by a group which contains and considers little to no input in the process" (de Long qtd. in Mueller, 2002, p. 285). But while frustration on this issue was great, it was small compared to concerns that the amendment effectively created a government monopoly in the domain name space. If a fee could be imposed for domain names, why was the task limited to NSI? If NSI had no competition, would there be a guarantee of a fair price? (Mueller, 2002)

Criticism of the NSF-NSI monopoly had to do with how the Internet's 'public' focus allowed governments, in particular the US government, to control aspects of the Internet. As described above, in addition to security, social and economic welfare is an important dimension of sovereign power. Although security and its 'restricted access' principles had been removed as the primary focus of network management, defining the Internet as a public educational resource meant that at some level the Internet's development remained rooted in sovereign institutions and priorities – hence the role of the NSF. Consequently, despite the NSF contributions to globalizing the Internet, it maintained a system of sovereign principles, which even if premised on *opening* access to a public good as the 'what' of Internet governance, still delimited government contractors as the 'who,' national agencies as the 'where' and a government monopoly as the 'how.'

---

[63] The DNS was initially design with seven generic top-level (g-TLDs) domain names: .com, .net, .org, .gov, .edu, .mil and .arpa. Non-generic TLDs usually refer to country-code top level domain names (ccTLDs), which are the two letter codes that usually signify a website related to a specific country (for instance, .ca for Canada). Given their connection with the education and the government, even after the imposition of the fee NSF continued to pay for registrations in .edu and .gov.

Commercialization undermined the 'public resource' approach for several reasons. First, as domain names were transformed from shorthands for information to portals for reaching global 'consumers,' buying and selling domain names became a profitable business in its own right. Therefore, limiting the sale, distribution, and even the number of top-level domain names to a single government monopoly prevented entry into a potentially lucrative industry. Also, in light of trademark concerns, NSI's distribution of names on the basis of first-come, first-served did little to address trademark protection. Given the exponential growth in demands for names in the .com space, the NSI argued that it didn't have the time to investigate competing name registration claims. An interview with an NSI staff member revealed, "If we had to research every request for a domain name right now, I'd need a staff of 20 people." In the absence of that, the NSI policy was "trademark problems are the responsibility of the requester" (qtd. in Quittner, 1994).

Second, the NSF was a national, sovereign authority. Allowing only a single agency (NSI) under its oversight to charge for domain names was interpreted as centralizing the root under the authority of the US government (c.f. Maher, 2006; Mueller, 2002). This stood at odds with the *worldwide* diffusion of Internet commerce: if e-commerce was indeed (re)structuring the Internet as a *global* marketplace, authority surely had to be more representative.

Cumulatively, then, the introduction of the Web and the commercialization of the Internet ushered in a vision of the Internet as a place for commerce, profit, and advertising. The Internet was no longer exclusively a public educational resource but also a *global* market. Despite this new global commercial focus, the NSF not only concentrated authority within a single government but did so in a government monopoly. Questioning the

appropriateness of the NSF as a managing authority for the domain name space was therefore a criticism of how sovereign influence prevented effective governance of the commercial Internet.

Incorporating the political vocabulary of 'competition'

The growing momentum behind the *global marketplace* both as a metaphor of globalization and as the Internet's discursive frame constituted a turning point in global Internet governance. As commercial activities became acceptable, the misappropriation of the first-come, first-served distribution of domain names and the creation of a monopoly in domain name registrations created a crisis of confidence in existing institutions and practices of global Internet governance. A viable *commercial* global Internet therefore required redefining the principles and objectives of Internet governance. In this section, I trace how the emergence of the *global marketplace* metaphor became the basis of a new political vocabulary that redefined the 'global' potential of the Internet. This vocabulary was incorporated into two related discussions. The first occurred within the technical community – the same set of users who had been instrumental in defining the IETF's standards process – which demanded that the NSF-NSI monopoly be dismantled and DNS management be moved to the private sector. The second was initiated through the US government's criticisms of the technical community's proposals, which it argued did not do enough to privatize DNS governance. The resulting confrontation reinforced the definition of the Internet as a global economic platform, with 'competition' the legitimating principle and trademark protection and privatization the central objectives of its governance.

From common pool to commodity: draft-postel, the IAHC-gTLD, and the competitive DNS

The incorporation of the *global marketplace*'s vocabulary within the technical community (comprised of ISOC, the IAB and some IETF participants) was initiated by a concern for 'open access.' The NSF's decision to impose fees for domain names effectively converted them from common-pool resources to profitable commodities. A government monopoly therefore *restricted* access by barring alternative registration centres, which could equally profit from DNS registrations, and potentially created price barriers if domain name registration prices were arbitrarily kept high.

Following the NSF's fee announcement, Postel, in a letter to the ISOC Board, asserted that "charging … for domain registrations was sufficient cause to take steps to set up a small number of alternative top-level domains managed by other registration centers." In his view there had to be "competition between registration services to encourage good services at low prices" (Postel qtd. in Mueller, 2002, p. 128). To explore the issue further, Postel and other members of the technical community set up an IETF Working Group on Shared TLDs. The working group's deliberations were published as a draft-RFC titled "New Registries and Delegation of International Top-level Domains" or '*draft-postel*' (Postel, 1996). Arguing that "there [was] a perceived need to *open* the *market* to *commercial* [TLDs] to allow *competition,*" it proposed an increase in the number of TLDs and number of entities ('registries') who could register domain names" (Postel, 1996; my emphasis). Specifically, *draft-postel* recommended the introduction of 150 new TLDs in the first year by creating fifty new TLD registries, each overseeing three of the new TLDs. In subsequent years, thirty

new TLDs would be introduced by allowing ten new registries to assume the responsibility for three new TLDs. Management of TLDs would be restricted to a five-year period, with the presumption that good service would result in contract renewal. All registry applicants would pay a $1000 application fee and successfully chartered registries would pay $10 000 and one percent of their annual revenues to a fund managed by ISOC for insurance against failed registries. This fund would also support IANA, which was to be the operational locus of this new TLD regime.

Although IANA had been performing various DNS policy functions with relative autonomy, it was still under US government contract. However, in response to NSF's domain name fees imposition, ISOC published a memo claiming that the "the rapid commercialization and globalization of the Internet" necessitated that the "responsibility for key central components of Internet infrastructure evolve away from support and oversight by the US government to an independent … basis" (Internet Society, 1995). Arguing that it better represented the interests of the global user community and could provide a more neutral authority, ISOC stated its intention to "take a formal role in the oversight and licensing of competitive registries for the … Internet name space, in support of the IANA and with the assistance of the IAB" (Internet Society, 1995).[64] It was "not proposing to provide direct operational services" but to take on the responsibility for "setting policy, providing administrative oversight and directly managing the selection of domain name providers for [gTLDs]" (Internet Society, 1995). ISOC's endorsement of *draft-postel* showed that leaders

[64] Based on the open process of the IETF-ISOC-IAB standards process, there was growing support for ISOC to take a lead role in DNS management. In particular, a meeting sponsored by the NSF on 20 November 1995 to address growing questions about who had the authority to manage the root in a global commercial context implicitly endorsed ISOC/IANA. They were considered to be the appropriate private agencies because ISOC's open participation structure gave voice to a diversity of opinions. It also prevented governmental involvement, i.e. through the ITU, which was feared might hinder competition (National Science Foundation & Harvard Information Infrastructure Project, 1995).

in the technical community were "backing a plan to assign *commercially* valuable *property rights* in top-level domains to *competing* registries, collect fees from licenses and in the process establish itself as the manager of the DNS root" (Mueller, 2002, p. 136; my emphasis). In short, IANA/ISOC argued that opening the DNS to competition required privatizing the root under their authority.

Private governance in the Internet sector was not a novel idea – the IETF is a private organization. However, under the influence of the *global village* metaphor, private authority was justified in order to ensure bottom-up, grassroots, and deliberative communications for an openly accessible Internet (i.e., by removing it from security agenda and governmental bureaucracies). While such goals were present in ISOC/IANA's claim for authority (because of its historical association with the IETF), in the emerging context of the *global marketplace*, they based their legitimacy on the need to foster competition. Were IANA/ISOC to take over management of the root, the IETF and its standards process would not be dismantled – indeed, *draft-postel* was the outcome of an IETF working group. As the Internet evolved, technical standards continued to be important. Therefore, the IETF's work would "[serve] the [TLD] administrative work in a technical capacity" (Postel, 1996).

Although it proposed a competitive and private alternative, *draft-postel* was criticized for providing an unfeasible framework for privatizing DNS management and promoting competition. The ITU argued that IANA/ISOC imposed a "tax on the root" and trademark holders worried that more TLDs would exacerbate domain name squatting and speculation. Alternative registries were perhaps the most disappointed, asking why, if the authority of the NSF to charge fees was in question, did IANA have the right to "dictate to people what fees or market forces are to cause TLDs to exist?" (Denniger qtd. Mueller, 2002, p. 139)

To formulate a more palatable solution, in February 1997, ISOC and IANA began the process anew, inviting its critics to join them in the 'International Ad Hoc Committee on Generic Top Level Domains' (IAHC-gTLD) and together formulate another privatization proposal.[65] This new set of recommendations treated the DNS as a "public resource … subject to public trust." Rather than allowing TLDs to be 'exclusively' held by single entities (i.e. .com belonged exclusively to NSI), they would be held in common by a limited number (28) of 'registrars', who could all register names in any TLDs. To balance trademark concerns with the desire to expand the name space, famous names would be removed from the available pool of names and only seven new TLDs would be introduced, a stark contrast to *draft-postel*'s proposals. Finally, a Policy Oversight Committee with representatives from ISOC, IANA, IAB, registrars, ITU, WIPO, and the International Trademark Association would oversee the system (International Ad Hoc Committee, 1997). Asserting its authority in a Memorandum of Understanding (IAHC-gTLD MoU), the IAHC said that its proposal would come into force when the NSF-NSI cooperative agreement expired in 1998. To give the MoU an aura of legitimacy, it was signed at a formal ceremony hosted by the ITU, as if it were an international treaty.

Criticism of the IAHC proposal was even more vitriolic than that of *draft-postel*. NSI claimed that it *owned* .com, .net, and .org, and would continue to do so after the expiry of the Cooperative Agreement, thus the IAHC had no authority to create new registries and registrars. Alternative registries argued that more TLDs were needed to ensure competition, and civil society groups raised concerns about the underlying assumption that a domain name was a trademark (see Mueller, 2002, pp. 146-151). With the exception of the concerns raised

[65] In particular, ISOC and IANA invited representatives from the International Trademark Association, the ITU and the World Intellectual Property Organization (WIPO), and even a representative from the US Federal Networking Council. Notable absentees were NSI and alternative registries.

by the civil society groups, these criticisms demonstrated that the issue was no longer about *whether* privatization, competition and trademark protection should be the focus of Internet governance but rather *how* it would be adequately introduced.

Effectively, efforts to delegitimate the NSF-NSI arrangement and enable broader participation in domain name distribution changed the criticism of sovereignty from concerns over security restrictions to the manner in which sovereignty, as expressed through a US government monopoly, restricted competition. The process also transmuted 'open access' from its reference to a non-commercial and public communications medium; instead, it came to designate the ability to compete in the domain name (market) space. With *competition* in the DNS now assumed as the priority objective and *privatization* as the appropriate means, the vocabulary of *commercialization* and *trademark protection* had been incorporated into the technical community's vision for Internet governance.

Territoriality to trademarks: the US government's Framework for Global Electronic Commerce

Despite the technical community's efforts to promote privatization and competition, formal authority over the Internet root remained with the US government. When ISOC endorsed *draft-postel*, a member of the Federal Network Council (FNC) wrote to the ISOC Board asking whether "ISOC is claiming that it has jurisdiction and overall responsibility for the top-level address and name space? If yes, how did ISOC obtain this responsibility; if no, then who does own it?" (Aiken qtd. in Mueller, 2002, p. 136) Mike St. Johns, DARPA's representative on the FNC, made a more direct claim to authority. At a meeting hosted by the

NSF regarding the privatization of the Internet root, St. Johns claimed that the US Department of Defense owned the root and that policy authority had been transferred to the FNC, who had delegated it to the NSF (qtd. in Mueller, 2002, p. 137). Yet despite sending signals to ISOC that its effort to privatize the root would be contested by the US government, little was done to stop ISOC/IANA's efforts. According to Mueller (2002, p. 140), although the FNC advisory council urged a transfer of policy authority from the NSF to "some appropriate agency," nothing happened. The IAHC-gTLD MoU, however, with the number and nature of its participants, compelled a response. Although the US government agreed that policy authority over the DNS should be privatized, it refused to endorse the IAHC-gTLD MoU. It argued that the proposal actually hindered effective privatization and therefore ran the risk not only of compromising competition in the DNS but the Internet's overall capacity for global electronic commerce.

The *global marketplace* was the central motif in the Clinton-Gore Administration's globalization *and* Internet policies. The prevailing view was that globalization was "fueled by a technological revolution that enables information, ideas and money, people, products and services to move within and across national borders at increasingly greater speeds and volumes" (Clinton, 2000). This view presented the Internet as one of globalization's central platforms and drivers. It was situated within the sentiment that the end of the Cold War has shifted the emphasis from security to the global economy. Under the rubric of the 'information superhighway', Vice President Al Gore asserted that that "the rationale for sustaining the 'national security state', in which most of the nation's technological investments funded by public money went to the military, has given birth to a new concern for 'national economic states' and the enthusiasm for high tech" (qtd. in CPSR, 1993).

Attention to the Internet was therefore about advancing research and education but also about creating new kinds of economic opportunities that would enhance US economic competitiveness in the global economy. Gore described the Internet not only as the infrastructure that made the new global economy possible but as the "most important and lucrative marketplace of the 21st Century" (Gore qtd. in Elmer-DeWitt, 1993).

To explore the Internet's economic potential, in 1995 President Clinton appointed Ira Magaziner to direct an *Interagency Task Force on Global Electronic Commerce on the Internet*. To develop policy recommendations, Magaziner consulted the Global Internet Project, a consortium of telecommunications executives who advocated the removal of "unnecessary international regulations and national laws that impede or inhibit the growth of the Internet" (Global Internet Project Website). Magaziner consequently asserted that private sector leadership was necessary to ensure the Internet grew as "an engine for free commerce."

This approach however had more to do with the 'cybermall' vision of the Internet and said little about competition in domain name space. DNS issues only caught Magaziner's attention after a series of high profile cases regarding the registration of famous names by individuals with no obvious connection to those names forced the US Trademark and Patent Office and the Department of Commerce to consider the relationship between domain names and trademarks. Based on these investigations, Magaziner concluded that "[ignoring] trademarks in the issuance of domain names ... could have a negative commercial impact" (Magaziner qtd. in Mueller, 2002, p. 156). The plot thickened when the NSF sought to extricate itself from domain name management by terminating its Cooperative Agreement with NSI early. Arguing that "the "Internet [was] no longer primarily a medium for the

exchange of information among computer networks in the scientific community," the NSF saw no reason to continue to provide support for registration services (Bordogna, 1997a; c.f. Bordogna, 1997b).[66] Ending the agreement early would have privatized the root exclusively under NSI, exacerbating concerns about monopoly power and trademark protection. To avoid this, Magaziner halted the NSF's exit and in March 1997 formed the *Interagency Working Group on Domain Names* to develop a more formal arrangement for transferring the root from the US government to the private sector.

Given Magaziner's emphasis on privatizing the root and protecting trademarks, the US government's rejection of the IAHC-gTLD MoU is puzzling. The Interagency Task Force refused to support the proposal on the grounds that "[international] organizations [such as the ITU] might have too great a role … and we won't have a private sector-driven process" ("U.S. rejects Name plan", 1997). The IAHC's treatment of the domain name space as public resource under public trust suggested heavy governmental regulation, similar to other telecommunications sectors in which the ITU played a large role (c.f. Mueller, 2002, p. 144). Specifically, there were fears that governments might try to regulate content, which would hinder competition and the free flow of Internet commerce. From the US government's perspective, then, the technical community and its IAHC proposal did not go far enough in promoting privatization. Ironically, although the IAHC was formed to remove sovereignty from the DNS by limiting US government involvement, the US viewed the IAHC-gTLD as a conduit for sovereign power.

[66] Bordogna, then Acting Deputy Director of the National Science Foundation, elaborated in this memo to the Inspector General that "[the Internet] has gone from the development stage to the application stage, and the administrative structure is presently sustained by the general purpose of the enterprise and by commercial participants. Because the operations that are covered by the Cooperative Agreement no longer require financial support from NSF and the expectations of the Cooperative Agreement have been fully met, we believe it is time for NSF to focus its attention on the next leading edge activities in this area" (Bordogna, 1997a).

On 1 July 1997 the US government issued a counter-proposal. The President's *Framework for Global Electronic Commerce* [*FGEC*] (*Framework for Global Electronic Commerce*, 1997) called the Internet a "vibrant global marketplace" and argued that its competitive potential required governance "by a consistent set of principles … across borders." This concern for commercial competition was directly linked to DNS management. Just as businesses operating in 'real space' required trademark protection in order to be competitive, the *FGEC* contended that on-line businesses required protection for their marks, particularly as they appeared in web addresses. Unlike conventional businesses, however, domain names transcend discrete territories, which created potential complications, since different countries could employ different legal requirements for domain names. To circumvent this, the *FGEC* proposed a system of global Internet trademark laws, allowing trademarks in domain names to be recognized across borders. Furthermore, domain names provided a form of business marketing, which created a global market for names. Without appropriate rules for competition in the DNS, the overall competitiveness of the global marketplace could be undermined – for instance, if a monopoly's prices for domain name registrations were too high. Accordingly, as an *FGEC* provision, the President directed the Secretary of Commerce[67] to "support efforts to make the governance of the domain name system *private* and *competitive* and to create a contractually based self-regulatory regime that

[67] Internet management at this time migrated from the National Science Foundation to the Department of Commerce, as the research/academic focus of the Internet was replaced with the view of the "Internet as a non-regulatory medium, one in which competition and consumer choice will shape the marketplace" ("Executive Summary of E-Commerce Report", 1997). The US government stated, "as the Internet becomes commercial, it becomes inappropriate for US research agencies (NSF and DARPA) to participate in and fund [Internet management]" (National Telecommunications Information Authority, 1998a). However, within a neoliberal market the directive was not one of shifting responsibility between state agencies but how the state would shift authority to the market. The Department of Commerce's role was, as stipulated by the Executive Order, to create effective self-regulating market mechanisms for managing the Internet. The institutional change, therefore, was a 'market directive,' an outcome *produced* and legitimated by the authority enshrined in the marketplace.

deals with conflicts on DNS usage and *trademark laws* on a *global* basis" (*Presidential Directive on Electronic Commerce*, 1997). In its rejection of the IAHC, the US effort to efface the legitimating power of sovereignty deepened the vocabulary of *competition*, *privatization,* and *trademark protection*, thereby reinforcing the *global marketplace* as the 'global framework' for Internet governance.

Thus, the incorporation of the *global marketplace* metaphor occurred through two main efforts. In the first, the technical community's challenge to the NSF-NSI monopoly over domain name registrations, inscribed *privatization*, *competition,* and *trademark protection* as the expected terminology of Internet governance. In the second, the US counter-proposal linked competition and privatization of the DNS to the broader commercial and consumer potential for global electronic commerce. For a *competitive* global consumer market, there had to be a *competitive* and global DNS, which required *privatized* governance and attention to *trademarks*. Although borne of disagreement, the two competing proposals actually deepened the inscription of the *global marketplace* metaphor.

This metaphor was explicitly juxtaposed against the normative force of sovereignty. Since government regulation prevented competition, the technical community argued that private agencies were needed to manage the DNS. In effect, 'commodity' and 'competition' were championed over 'public resource' and 'social welfare,' and 'private authority' came to replace 'government.' This shift further displaced the *global village* metaphor by transforming open access from a principle of 'global communications' to one of 'global competition.' Paradoxically, although the US was the target of the IAHC-gTLD effort to eliminate sovereignty, the US rejection of the IAHC-gTLD and its counter-proposal broadened the criticism of sovereign power: if competition required privatization, the

globalization of the Internet as a commercial platform required removing governments altogether. Accordingly, the *FGEC* asserted that privatization, competition, and trademark protection had to be constructed "across borders" on a "global basis."

Although reconciling the US and IAHC-gTLD positions would take time, their agreement on the need to privatize DNS management demonstrates how the *global marketplace* metaphor shaped the Internet's global potential. Both sides assumed that competitive commerce was the 'why' of global Internet governance. Within the domain name space, this translated into creating a global market for domain names as the 'what,' a private authority as the 'who' and 'where,' and a global body of trademark law the 'how' of governance.

Defining roles and responsibilities: the 'Green Paper,' the 'White Paper,' and the consolidation of ICANN

Ultimately the impasse between the IAHC and the US government was about what kind of private authority would promote competition in the domain name space and which actors would be involved. With their different evaluations of sovereign power, the resolution to this debate rested on which of the proposals – the IAHC-gTLD or the *FGEC* – would establish the terms of reference for DNS management. Terms of reference for governance are established when a metaphor's descriptions become the vocabulary that defines political reality. These terms redirect actors' identities and activities to form a network of action in support of the political order's legitimating principles. In time, this network produces a given political order's distinctive governance institutions. In this section, I describe how the NSI's

monopoly and the diversification the Internet user community undermined IAHC efforts to implement the gTLD-MoU, leaving the *Framework for Global Electronic Commerce* as the basis for privatizing the DNS. After convincing its critics to support its proposal for a new private non-governmental corporation, the US government set the context for the formation of the Internet Corporation for Assigned Names and Numbers (ICANN). Endorsed by the US Department of Commerce as the agency responsible for creating a global market for top-level domains, ICANN emerged as the visible expression of the 'who' and 'where' of a privately-governed, competitively-driven global Internet.

On the heels of the Presidential Directive, the National Telecommunications and Information Agency (NTIA) in the Department of Commerce issued a public request for comments entitled "Improvement of Technical Management of Internet Names and Addresses; Proposed Rule" (National Telecommunications Information Authority, 1998b). Based on the comments received, the NTIA outlined the US government's privatization plan in a 'Green Paper': "A Proposal to Improve the Technical Management of Internet Names and Address" (National Telecommunications Information Authority, 1998a). The Green Paper advocated the creation of a "private not for profit corporation" that would set policy on the allocation of IP addresses, oversee the operation of the Internet root, and determine the criteria for adding new gTLDs. The proposal stressed the importance of both competition ("Where possible, market-mechanisms that support 'competition' and consumer choice should drive the technical management of the Internet") and 'privatization' ("private sector is preferable to governmental control"). It also suggested the limited introduction of gTLDs to balance the desire for increased competition in the domain name space and the need for businesses to "have confidence that their trademarks can be protected" (National

Telecommunications Information Authority, 1998a). Although many of the Green Paper's recommendations resembled those of the IAHC-gTLD MoU, it did not acknowledge the Ad-Hoc Committee's efforts.[68]

Observing that "as a legacy major components of the domain name system are still performed by or still subject to agreement with agencies of the US government," the US government claimed responsibility for ensuring a stable and risk-free transition to a private system for DNS management (National Telecommunications Information Authority, 1998a). The Green Paper therefore stipulated that the US government would retain policy oversight of the new corporation until September 30, 2000, when that entity would have presumably proven its ability to independently manage the DNS. Furthermore, as the root's technical administration occurred in the US, the new corporation would be incorporated under US law as a not-for-profit entity.

Although it put forth a privatization proposal, the Green Paper was criticized for centralizing the root under the US government. Opponents claimed that it was hypocritical to place a strict prohibition on participation of governments in DNS management while giving the United States exclusive authority to oversee transition to a private authority. Moreover, the Green Paper only transferred *policy* authority to the new corporation. The root zone file itself would remain the property of US government. The European Commission charged that "the US Green Paper proposals appear not to recognize the need to implement an international approach … The US proposals could, in the name of globalisation and

[68] Unlike the IAHC-gTLD MoU, the Green Paper proposed to separate registry and registrar functions in order to create competition in the second-level domain name space. Although public comments had strongly supported a competitive registrar function, there was significant scepticism about competing registries. As domain names, now becoming brands, were hard to change, there was concern that registries could create lock-in costs that would do more to hinder rather than promote competition. The US government saw this as a minimal concern, arguing that registries, in order to be competitive, would avoid such practices (National Telecommunications Information Authority, 1998a).

privatisation of the Internet, consolidate permanent US jurisdiction over the Internet as a whole" (qtd. in Mueller, 2002, p. 165). For the IAHC, the US government's assumed legacy role reinforced its claims that US involvement impeded broad-based DNS management. The IAHC cited the Green Paper as evidence that the US government "continues to miss the point that the rest of the world and its governments think that the Internet is a global resource, rather than strictly belonging to the US" (qtd. in Mueller, 2002, p. 159).

Objections to the Green Paper galvanized support around the IAHC-gTLD MoU (Mueller, 2002, p. 165). Several factors, however, hampered the IAHC's efforts and prevented them from getting off the ground. At a purely functional level, operational control of the root lay with the NSI, whose desire to maintain monopoly control over gTLDs meant it was unwilling to cooperate with the IAHC.[69] Without NSI's support, the IAHC had neither the authority nor the ability to make changes to the Internet's root-zone file. The IAHC was also unable gain the support of the global Internet user community that it purported to represent. By making significant concessions to trademark interests, it lost the support of those users who argued that limiting the number of gTLDs to avoid trademark violations reduced competition (i.e. alternative registries). More than this, however, the IAHC leadership failed to recognize that the 'user' community itself had changed. Commercialization of the Internet had introduced business interests from the telecommunications sector as 'users' (Mueller, 2002, pp. 163-164). Suspicious of its 'public trust' approach to the domain name space, and apparently for its arrogance, business did not

[69] In 1996, Paul Garrin, operator of Name.Space, asked NSI to include alternative top-level domain names hosted by Name.Space in the Internet root. Not doing so would be viewed as anti-competitive so NSI deferred the question to IANA. Unaware of any authority it had regarding this decision, IANA refused to accept responsibility, and NSI subsequently asked the NSF for guidance, and asked that it add the Name.Space TLDs. NSF rejected the request on the basis that it needed to better understand the governance authority issues raised by the issue. It also requested that NSI not add any new TLDs until the NSF had finished consulting on the issue with other US government agencies (Mueller, 2002: 153). Presumably, even if NSI had agreed to cooperate with the IAHC, the IAHC still would have had trouble adding new TLDs to the Internet root.

support the IAHC-gTLD MoU (Mueller, 2002, p. 171). In the end, with neither the support of NSI nor the ability to cater to diverse interests inside the global user community, the IAHC was left with little ability to implement its privatization proposal.

By default, the Green Paper became the nodal point for discussions about Internet governance. Aware that the Green Paper had not reconciled stakeholder differences, Magaziner undertook discussions with the US government's major critics, hoping to find a common ground that would secure their support for the Green Paper's privatization plan. Achieving consensus on the nature of the new corporation required reconciling differences between the ISOC/IANA, national governments, and the US government. Furthermore, because telecommunications businesses were heavily invested in the success of Internet commerce, Magaziner also needed to bridge differences between ISOC/IANA and the business community.

Not only was ISOC/IANA concerned that the US claim over the root gave undue power to a single government, the Green Paper further advocated privatizing the functions performed by IANA and transferring them to the new corporation.[70] Magaziner, however, realized that the technical community held the historical knowledge and expertise for performing these functions, and after extended discussions with IAB members, conceded that any new corporation would have to include IANA if the transition was to be technically sound (c.f. Drezner, 2004, ft. 82). Having their authority acknowledged and given a central role in the management of the root, lessened ISOC/IANA's fears about US government influence over the domain name space. Given the failure of the IAHC, though, the technical community also realized that it had to come to terms with the US government's initiative (c.f.

[70] The Green Paper did not refer to IANA as a corporate entity. Instead, it described IANA as a set of functions operating under US authority: "The US government would transfer existing IANA functions … to this new not-for-profit corporation" (National Telecommunications Information Authority, 1998a).

Mueller, 2002, p. 171). Postel and then IAB Chair, Brian Carpenter, thus formed the IANA Transition Committee to discuss IANA's integration into the Green Paper's governance structures. Based on Magaziner's previous consultations with them, business interests had already endorsed the Green Paper. Also, many members of the technical community had moved from government and academia to work in the in telecommunications sector, which allowed for informal dialogue that bridged differences between the technical community and business, lending further support to the new corporation proposed in the Green Paper (c.f. Mueller, 2002, p. 171).

The support of other governments, in particular the European Union, had yet to come. Concerned about American dominance of the Internet sector, the EU supported dismantling the NSI monopoly to prevent a US-based entity from having undue influence in the domain name space rather than simply to ensure competition (Drezner, 2004, p. 495). One of the EU's major criticisms of the Green Paper was that incorporating the new corporation in the United States might make US trademark law the default legal framework for the domain name space. To guard against this, the European Commission insisted that WIPO be given the responsibility to handle trademarks. After extended discussion, the US government accepted the EU's demand. In turn, US demands to exclude the ITU were not contested (*). Because competition, privatization, and trademark protection were not disputed as general principles, Magaziner was able to get those who had initially opposed the Green Paper to become invested in its success. As these common interests were established, NSI, alternative registries, smaller ISPs, and users remained at the periphery of the process. With their desires to maintain monopoly power or to challenge trademark provisions, these groups' agendas failed to cohere with the Green Paper's objectives (c.f. Mueller, 2002, p. 172).

Due to Magaziner's efforts, the delineation of the new corporation in the 'White Paper' on the "Management of the Internet Names and Numbers" represented a consensus among the US government, IANA/ISOC, business, and the EU about privatizing the management of the DNS. Unlike the Green Paper, the White Paper acknowledged the efforts of the IAHC process, and praised it for "[introducing] a unique and thoughtful concept for the DNS administration" (National Telecommunications Information Authority, 1998c). Moving forward with privatization, however, would require concrete actions. Successful recruitment requires that actors redirect their activities to take on roles and responsibilities in support of a new political order. In the DNS debates, the negotiations that produced consensus involved agreeing to how different actors would assume responsibilities for the tasks required for privatization and competition. The White Paper thus reflected how the US government's initial detractors' roles were redirected and redefined in the effort to privatize the governance of the domain name space.

Although the White Paper listed a variety of different tasks, three in particular reflect how the debates around the Green Paper developed responsibilities that would implement the US government's privatization principles. The first and most obvious was IANA's incorporation into the new governance system. Acknowledging that IANA performed important policy functions regarding the technical development of the domain name space as a government contractor, the White Paper saw no reason why IANA itself "could not be reconstituted by a broad-based representative group of Internet stakeholders or that individuals associated with IANA should not themselves play important foundation roles in the formation of the new corporation." (National Telecommunications Information Authority, 1998c) The White Paper, then, redefined IANA from a government contractor

administering a *public* resource to the 'foundation' and operational locus of the new *private* corporation.

The second redefinition related to the role of governments. To avoid the influence of sovereign governments in DNS management, the White Paper divested governments of formal decision-making authority. Leaving no room for interpretation, and making an explicit statement against the ITU, the White Paper held that "neither national governments acting as sovereigns or *intergovernmental organizations* acting as representatives of governments should participate in the management of Internet names and addresses" (National Telecommunications Information Authority, 1998c; my emphasis). To the degree that these groups could participate, it would be "as Internet users in a non-voting advisory capacity" (National Telecommunications Information Authority, 1998c). Power would be located in a board of directors constituted by representatives from regional and IP address registries, the IAB, domain names registries and registrars, the Internet user community, and the CEO of the new corporation (National Telecommunications Information Authority, 1998c). To allay critics' concerns about US control over the domain name space, the White Paper reiterated that the US government would only "continue to participate in policy oversight until … the new corporation was established and stable" and it would "ramp down its cooperative agreement with NSI with the objective of introducing competition into the domain name space" (National Telecommunications Information Authority, 1998c). Excluding governments from decision-making and putting conditions on US government involvement therefore met the dual concern about the undue influence of the US government and the role of governments in general as the means by which sovereignty impeded competition in the DNS.

The third recasting of responsibilities reflected the US government's concession to give WIPO the job for developing rules regarding trademark protection. The White Paper, like the Green Paper, maintained that the Internet's commercial success required that businesses be able to trust in trademark protection, and that since cyberspace could not be easily carved into national jurisdictions, ensuring such confidence required a more uniform, borderless legal framework. WIPO was thus asked to consult with both trademark holders and Internet users who did not hold trademarks and develop recommendations for a uniform dispute resolution mechanism to deal with instances of cyberpiracy and protecting trademarks in the gTLD space. It was also asked to evaluate the consequences of introducing new top-level domains for trademark holders. WIPO itself would not manage trademarks in the DNS but would forward recommendations to the new corporation's board, which would make final decisions on how trademark protection would be implemented.

According to Mueller (2002, p. 172), the US government " … had learned from the reaction to the Green Paper [that] it had to stay in the background rather than the foreground." Thus, the White Paper reflected its effort to "impose some basic principles and constraints on the process and serve as guarantor of the emerging institution's stability, but defer key policy decisions to the new entity." This explains why the White Paper specified different roles and responsibilities only, rather than stipulating a new formal corporate entity, and why, unlike most White Papers, it was a non-binding statement of policy. It only provided the parameters for a new corporation – i.e., that it be based in the United States, that it should ensure user participation, that governments were not allowed to sit on the board, etc.

Beyond this, the US government called on the 'private sector' to come to a consensus about the new organization, and recommend it to the US government.[71]

To kick-start the discussion, the US government initiated the 'International Forum on the White Paper' (IFWP), which brought together IANA/ISOC, civil society groups, business, and number of other interested parties to determine the shape of the new governing body. However, differing interests made consensus difficult. Moreover, the White Paper stated that because of IANA's expertise, "private sector organizations will want Dr. Postel and other IANA staff to be involved in the new corporation" (National Telecommunications Information Authority, 1998c). With this endorsement, IANA defected from the IFWP and set about creating its own proposals for the new corporation.

Deferring to the authority of the diverse groups in the 'private sector', the IFWP also gave voice to critics of trademark protection and those who advocated human rights issues. Yet trademark protection was a central objective of the new corporation, and the incorporation of WIPO signalled its institutionalization into the new governance regime. The White Paper also stated that the new corporation would only address "the management of names and addresses … Existing human rights and free speech protections will not be disturbed and therefore, need not be specifically included in the core principles of DNS management" (National Telecommunications Information Authority, 1998c). Although the IFWP was supposed to foster discussion within the White Paper's parameters, instead it

[71] Specifically, the US government stated that steps to facilitate the transition to the new corporation "will need to be taken by the private sector. For instance, a new not-for-profit organization must be established by the private sector and its Interim Board. Agreement must be reached between the US Government and the new corporation relating to the transfer of the functions currently performed by IANA" (National Telecommunications Information Authority, 1998c).

resulted in a debate about the White Paper's objectives itself. Consequently, the IFWP fell into disarray and was eventually disbanded.[72]

As the different private sector groups failed to reach consensus, the US government received several competing proposals for the new corporation. Jon Postel's IANA-coalition proposed ICANN. Because ICANN had a ready-made set of by-laws and an (self-selected) interim board of directors, Magaziner approved its proposal to keep the privatization process from stagnating. To redress concerns raised during the proposals' public comment period about the transparency of ICANN's decision-making process and the participation of users, Magaziner directed ICANN to negotiate with its critics. The intent of these negotiations was not to create a new proposal. Having approved ICANN, Magaziner had established it as the institutional structure for private DNS management. ICANN's negotiations with its critics would therefore be about reforming the ICANN framework rather than creating a different corporate framework. On 25 November 1998 ICANN entered into a Memorandum of Understanding (*MoU*) with the Department of Commerce and on 26 February 1999 was recognized as the new private corporation for DNS management. According to the terms of the *MoU*, policy authority would be fully transferred from the US government to ICANN in 2000, assuming a stable transition to a private governance system had taken place.

The popularization of the Internet as a *global marketplace* and the resulting discussions about a market for domain names culminated in ICANN. When public attention addressed this new area of global Internet governance, ICANN was described as the "Internet's new oversight body… beginning to make decisions and shape policy that could ultimately affect everyone who uses the global network" (Clausing, 1999; c.f. Nuttall, 1998).

[72] For a more detailed discussion of the IFWP process, see Mueller (2002, pp. 174-184; 197-201).

According to *New York Times*, ICANN "[cleared] the way for the global Internet to be governed without governments" (Harmon, 1998).

'Private' performances: privatization and the ratification of competition

As the new private corporation for DNS governance, ICANN was responsible for developing procedures that would create and maintain a competitive global market for top-level domains. Because these procedures were designed to ensure competition, they were more than the functional tasks for the day-today operation of the DNS. Rather, they had to ensure that competition remained the core objective – the legitimating principle – of DNS policy. ICANN's operational procedures therefore signified a set of governance practices that not only regulated a global market for domain names but also reinforced the definition of the Internet as *global marketplace*. Again, my analysis focuses only on the initial stages of ICANN's development – just before the expiration of the its original *MoU* in 2000. Since then, ICANN's operations and relationship with the US government have continued to evolve. My goal is only to highlight the influence of *global marketplace* metaphor in shaping ICANN and its governance practices in their 'founding moment.'

ICANN developed its initial operational procedures in the *MoU* (U.S. Department of Commerce & Internet Corporation for Assigned Names and Numbers, 1998), its *Articles of Incorporation* (1998a), its bylaws (1998b; , 1998c; , 1999a; , 1999b), and its *Uniform Dispute Resolution Policy* (2000). In all, competition was unequivocally the primary objective of DNS management. For instance, the *Articles of Incorporation* stated that ICANN's purpose was designed to "[lessen] the burdens of government" in order to "enable

competition and open entry in Internet-related markets" (Article 3, Article 5). Of the procedures outlined in these documents, three in particular vividly demonstrate how ICANN's DNS management supported the Internet's commercialization by enabling and embedding competition in the domain name space.

The first relates to the role of governments. Article V of ICANN's bylaws expressly stated that "no official of a national government or a multinational entity established by treaty or other agreement between national government may serve [on the Board of Directors]" (1998b). Government participation was thus limited to a "Government Advisory Committee" or 'GAC' (1998b: Article VII, Section 3a) to be constituted of "representatives of national governments, multinational governmental organizations and treaty organizations" and would only "provide advice on the activities of [ICANN] as they relate to the concerns of governments" (1998b: Article VII, Section 3a). If ICANN was committed to preventing the subversion of global competition by parochial national interests, one wonders why governments were given a role at all. ICANN, however, was sensitive to the importance of the Internet in public policy, which would both affect governments and require their input. The GAC was therefore a forum where governmental concerns could be discussed. By involving states in an advisory capacity, the GAC would allow ICANN to be aware of inevitable interactions between its policies and national legislation and international treaties but circumvent the need for direct governmental action.

A second set of procedures implemented a borderless system of trademark protections for domain names. ICANN's responsibility for "[developing] policies … under which new top-level domains are added" (1998a: Article 3) had to, according to the *MoU*, consider the "effects of adding new gTLDs … on trademark … holders" (U.S. Department of Commerce

& Internet Corporation for Assigned Names and Numbers, 1998: Section C, 9d). To do this, on 24 October 1999, ICANN implemented the *Uniform Dispute Resolution Policy* (*UDRP*), which made arbitration mandatory when a registrant registered a name similar to a famous name that s/he had no rights to, or that s/he intended to use in bad faith – for instance, for sale back to the trademark owner or for defamation (Internet Corporation for Assigned Names and Numbers, 2000: Article 4a).[73] In all such cases, rights lay with the owner of the famous name. Moreover, anyone anywhere could question a registrant's right to a particular name in the DNS. Accordingly, DNS trademark arbitration and rules were not confined to national legal jurisdictions. If a competitive and global market required a global system of trademark regulations, the *UDRP* facilitated its operation in the DNS.[74]

ICANN's procedures for enhancing user participation are the third example of how the commercial scope of the global Internet was reinforced. The White Paper noted that "an increasing percentage of Internet users reside outside of the US, and those stakeholders want to participate in Internet coordination." Thus one of privatization's goals was to "ensure that the increasingly global Internet user committee has a voice in decisions affecting the Internet's technical management" (National Telecommunications Information Authority, 1998c). For this reason, ICANN's initial proposal was criticized for insufficiently involving individual users, and it was force to revise its bylaws to make provisions for the election of nine 'at-large' members (individuals) who would sit on the ICANN board.[75]

---

[73] This was made mandatory in two ways. First, implementing the *UDRP* was made a condition of registrar accreditation. Second, in their contracts with registrars, registrants had to agree to the terms of the *UDRP*.

[74] Some argue that ICANN's protection of trademark interests can also be seen through its slow introduction of new TLDs and the limited number introduced. It was almost three years before new gTLDs (seven in total) were added to the DNS and when they were, ICANN encouraged registries to invoke 'sunrise' procedures that would allow owners of famous names to register them in the new TLDs before registration opened to anyone else (Mueller, 2002, p. 193).

[75] Other board members were chosen to represent each of ICANN's different 'supporting organizations' (discussed below) by the board based on nominations put forward each supporting organization.

The focus on the Internet's commercial activities, though, shifted attention away from *individual* users. The conventional definition of users as individuals assumed that the Internet was a 'people-to-people' communications medium and represented a way to restrict government and corporate influence in the standards-making process. Indeed, IETF participants came to the IETF as individuals, not as representatives of other entities. The White Paper, however, argued successful Internet commercialization required more than the participation of individuals, pointing to the IAHC's failure to include business interests as its downfall.[76] Thus, when the White Paper proposed a structure for the new corporation's board that would include users, it defined individuals, as well as registrars, trademark interests, and business as 'Internet users'.

As ICANN tried to accommodate the growing diversity of the Internet's user community, while at the same time ensuring competition, individual users were systematically excluded. The structure of the Domain Name Supporting Organization (DNSO) is a key example. To address the concerns of different interest groups, ICANN was structured around a series of Supporting Organizations (SO), each of which addressed an issue related to the management of the DNS and made recommendations to ICANN's board of directors. As defined in the bylaws ratified on 6 November 1998, the DNSO was "composed of representatives from name registries and registrars of top-level domains … business and another entities that are users of the Internet." (Article VI, Section 3(a)iii). Measures adopted in revised bylaws on 31 March 1999 showed that enlarging the user community to accommodate commercial interests actually limited individuals' participation.

[76]The White Paper noted that "although the IAHC proposal gained support in many quarters of the Internet community, the IAHC process was criticized … for being dominated by the Internet engineering community, and for lacking participation and input from business interests and others in the Internet community" (National Telecommunications Information Authority, 1998c).

The revised bylaws restructured the DNSO around seven constituencies, none of which included individual users (Article VI-B).[77] Although a new 'General Assembly' was attached to the DNSO, allowing individual participation, this body only made recommendations to a DNSO Naming Committee, and did not contribute directly to decisions forwarded to the ICANN board.

Partiality towards commercial users over individuals became more apparent in the in the failure of the at-large elections. As the IFWP revealed, a number of users' interests were opposed to ICANN objectives, rejecting artificial scarcity and trademark protection in the domain name space or insisting that more attention be paid to human rights issues.[78] Although opposed to key ICANN objectives, these users still opted for participation. Realizing that these users could be elected to the board and compromise interests and approach of ICANN's existing directors in promoting trademark protection and competition, ICANN directors took steps to subvert the elections. First, to avoid the rights granted to voting members of a California not-for-profit corporation to scrutinize a corporation's records and accounts, the ICANN board designated the at-large election procedure as a board *resolution* and not a formal bylaw. Second, when ICANN's fears were realized and some of its critics were elected to the board, ICANN declared the elections a failure, citing an insufficient number of voters "to meet any test of democratic elections" (Roberts qtd. in

[77] These constituencies initially included: 1. ccTLD registries; 2. commercial and business entities; 3. gTLDs registries; 4. ISP and connectivity providers; 5. non-commercial domain name holders; 6. registrars; and 7. trademark and other intellectual property and anti-counterfeiting interests (see 'Bylaws for Internet Corporation for Assigned Names and Numbers: A California Nonprofit Public Benefit Corporation, As Revised March 31 1999. Available: http://www.icann.org/general/archive-bylaws/bylaws-31mar99.htm [accessed 22 March 2008]).

[78] In 2000, the Civil Society Internet Forum (CSIF) was convened to issue civil society perspectives on ICANN and its position on issues for the upcoming election. In its statement, the CSIF advocated against "Artificial Scarcity in domain names and centralization of DNS administration" and held that "intellectual property rights should not be privileged over other rights." Chastising the White Paper, it asserted that "US policy [had] been predominantly oriented toward commerce … [but that] Internet policy should be equally guided by other relevant principles, [such as freedom of expression" (Civil Society Internet Forum, 2000).

Hofmann, 2005, p. 13). Yet nearly 170 000 individuals voted.[79] According to Hoffman (2005, pp. 13, ft. 18) "representative voter participation on a global scale had never been the declared aim; it first gained acceptance as an assessment criterion after the election." Although ICANN commissioned a study to better develop at-large participation, none of its recommendations were included. Given their efforts to minimize the involvement of individual users, many saw the study as evidence that the "very existence of the at-large membership was up for examination" (Mueller, 2002, p. 201). The elections were never repeated and at-large users remained, as it were, 'at-large.'

According to Mueller (2002, p. 198), the DNSO constituency structure allowed ICANN to " [magnify] the … power of business, trademark and registrar groups and [minimize] or [eliminate] the influence of … non-commercial users and individuals," an intention further made evident the effort to undermine the at-large elections. Evidently, commercialization of the Internet diversified the identity of users, but also privileged a particular kind of user.

Thus, the advisory role of governments, the *UDRP,* and the privileging of commercial users all had a governance function. Privileging commercial users put commercial concerns at the forefront, which then supported the *UDRP*'s 'borderless' framework for managing trademark issues in the DNS. Both curtailed the explicit action of governments, whose interests did not always support the need for borderless commerce and competition. The advisory position of governments, in turn, reinforced the notion that competitive global commerce – both in the DNS and more generally – should have limited government involvement and privilege private authorities. The delineation of these practices in the *MoU*,

[79] Ironically, in the immediate aftermath of the elections, ICANN was heralded as being evidence of the possibility of democratic global governance (H. Klein, 2001).

ICANN's *Articles of Incorporation*, its bylaws, and the *UDRP* therefore not only described how ICANN's governance system worked – more significantly, it prescribed what was necessary for ICANN to maintain competition in the DNS space. By preventing direct government involvement, generating a global system for trademark protection in the DNS, and limiting the participation of individual users, ICANN ensured that this competition could not be subverted and guaranteed that the DNS remained a structured as a global, commercial, competitive, trademark friendly market. Such a market mandated private authority and thereby sanctioned ICANN as the legitimate authority for DNS management.

These governance practices also had a broader effect. Without the commercialization of the Internet, there would be no need to ensure competition in the domain name space – as the *Framework for Global Electronic Commerce* stated, commercialization of the Internet and competition in the DNS were interrelated. Therefore regular adherence to ICANN's governance practices not only structured the DNS as a global market but also reinforced the definition of the Internet as a *global marketplace*. As ICANN's governance of the DNS became routine, so did the definition of the Internet's global space as a commercial zone.

Moreover, privatization was also the performative logic underlying the *global marketplace* metaphor. Privatization, as shaped by the neoliberal ethos of the *global marketplace* metaphor, relegated governments to advisors, not regulators, implemented robust trademark protections that transcended sovereign jurisdictions, and privileged commercial users over individuals. It therefore guaranteed that the DNS was a commercial space and that it operated on a global scale. In other words, privatization was both a political objective and a mechanism of governance. It was not only the goal – it operationalized ICANN's system of DNS management as a competitive and global enterprise.

Ultimately, ICANN resulted from the inscription of the *global marketplace* metaphor in global Internet governance discussions. Given the task of creating and maintaining a competitive market for domain names ICANN's everyday activities were imbued with a normative agenda. As outlined in the *FGEC*, a competitive DNS would ensure that the Internet was amenable to global commerce. Since metaphorical inscription works through the production *and* performance of facts, ICANN ensured that privatization, commercialization, and trademark protection were features of the 'global' Internet. To this end, the cumulative effect of its emphasis on competition ('why'); its creation of a global market for domain names ('what'); the authority granted to its Board of Directors and commercially oriented Supporting Organizations ('who'); and its governmental advisory roles, the *UDRP,* and the limited participation of individual users ('how') reinforced the idea that the Internet was a borderless, commercial platform. And, to the degree that the DNS became a global marketplace, ICANN was sanctioned as the appropriate site ('where') for maintaining it.

Competing with 'competition': foreclosing sovereignty and 'open access'

The *global marketplace* metaphor normalized a new set of facts for global Internet governance. Defining the Internet through the political vocabulary of *commercialization*, *privatization,* and *trademark protection* made *competition* the legitimating governance principle. This vocabulary also recruited different actors into a network of action – consolidated as ICANN – and delineated governance routines that normalized the Internet as a commercial platform, necessitating a competitive market for domain names. However, since power operates relationally, the *global marketplace*'s ability to influence this outcome

required delegitimating and thereby displacing the normative force of both the *state of nature* and *global village* metaphors, along with their respective inscriptions of sovereignty and 'open access.'

The marginalization of sovereignty occurred in three phases. First, critics denounced exclusive US control over the DNS and attempted to privatize the root through the proposals outlined in the gTLD-MoU. For its part, the US government agreed to remove itself from exclusive management of the DNS but also decried the involvement of all governments, rejecting the IAHC privatization proposal due to the prominent role accorded the ITU. Despite their opposition, both positions reinforced the idea that successful competition in the DNS required non-sovereign governance institutions.

The second phase of sovereignty's displacement was evident as governments and other non-state actors authorized a new private corporation to make DNS policy decisions. This new corporation defined governments and intergovernmental organizations as 'users' rather than regulators. In the final phase, ICANN's operational guidelines relegated governments to an advisory position. Governments were participants in the ICANN system – however, their roles and responsibilities were no longer articulated through sovereignty. Instead, with competition as a primary objective of global Internet governance, governments became subsidiary actors supporting a privatized regime.

In short, while sovereignty initially defined the Internet through security impulses and then later as a public resource where governance authority lay with government contractors, the *global marketplace* metaphor disrupted this system with a new vocabulary of deterritorialization. *Territory* disappeared as a signifier of political governance as the 'borderless' economy replaced national economies and become embodied in the Internet. The

Internet therefore was *populated* with global consumers. Creating a competitive market *authorized* private institutions and *recognized* a global system of rules and legal frameworks.

Sovereignty's marginalization was accompanied by the displacement of the *global village* metaphor, which had inscribed 'open access' as the governing logic of the global Internet. The commercialization of the Internet as a *global marketplace* disrupted the Internet's function as a non-commercial and non-proprietary public communications medium. With new enthusiasm directed towards customers, commercialization transformed domain names from common-pool data locators to lucrative real estate. Interestingly, 'open access' was used to contest the NSI monopoly over domain names. The end effect, however, was to legitimate competition, rather than to further a communications agenda, demonstrating the growing popularity the *global marketplace* metaphor. 'Open access' was further disrupted as the definition of users was expanded to include individuals as well as business, trademark holders, domain name registries and registrars, and even governments. While initially, this may have signalled a broadening of the Internet user base, it actually privileged commercially oriented users. ICANN's restructuring of the DNSO with no provisions for individual users and the failure of the at-large elections demonstrate this shift. The legitimating power of 'open access' was further displaced as human rights issues and criticism of trademark protection were excluded from the DNS management agenda. Admittedly, ICANN was designed to protect trademarks so the initial effort to ensure 'open access' to the DNS market by limiting trademark protection was obviously pushed aside. Nor did ICANN intend to violate human rights – as the White Paper stated, free expression and free speech would be not be disturbed and therefore did not need to be included within

ICANN's governance objectives.[80] However, ICANN's focus on competition clearly shows that the *global village* was no longer the only way to understand the Internet's global potential. The acceleration of the Internet's globalization under the *global marketplace* added different political goals to the Internet governance agenda and, for specific issues, legitimated a different set of global Internet governance institutions and practices. While the popularity of the *global marketplace* metaphor did not efface the *global village* or eliminate its proponents, it did alter the *priorities* of global Internet governance.

Alternative explanations: ICANN as the manifestation of scarce resources and sovereign power

That the *global marketplace* metaphor was consequential in the development of ICANN is contested in two ways. The first is implicit, contained in the Mueller's (2002) theory of economic scarcity and institutional formation. As stated, Mueller's account is the seminal study of ICANN, detailing the major events, actors and issues that precipitated a change in the overall objectives and frameworks of Internet governance, not only within the US government but more globally. In his account, any common pool resource,[81] in this case IP addresses and domain names, are victim to a competition over property rights. Although IP addresses and domain names were initially available on a first come-first served basis, once taken, they were no longer available for others for use. Mueller therefore asserts that the

[80] Whether ICANN's DNS policies leave free speech and free expression untouched is debatable. ICANN has repeatedly rejected a proposal to create a new TLD – '.xxx' – that could be used to host pornographic websites (the most recent disapproval was in March 2007). Many pointed to this as evidence of the way ICANN's decision did, in fact, disturb free expression on the Internet (*).

[81] A common pool resource refers to a good in which restricting use is difficult, but use by one actor or group makes it less available to others. It differs from a 'commons' in which use by one group does not prevent use by others.

proprietary conflicts that resulted in the rush for domain names were inevitable, with the semantic value accorded to domain names through the popularization of the Internet through the World Wide Web and the privatization of the NSFNET backbone exacerbating these quarrels. Consequently, new rules and institutions would be needed to manage competing claims. ICANN is therefore the outcome of actors' self-interest in gaining and maintaining property rights in an (global) economy of scarce resources.

But Mueller presents a tautological argument. Rather than accounting for the shift to marketization, Mueller assumes that the market logic – that actors will compete to own limited resources – has always been implicit in Internet governance, specifically in the domain name space. This assumption is problematic given that the Internet, in the heyday of the IETF and its technical community of users, was decidedly not a marketplace. This was reinforced by the NSF's prohibitions on commercial use of the NSFNET, and the IETF's non-proprietary standards development culture. Indeed, at some level the first-come, first-served principle can be seen as a normative commitment guarding against assigning 'market' value to domain names. Allowing domain names to be allocated on a first-come, first-served basis would prevent the differential valuation of names and numbers, averting proprietary demands and conflicts. All names were equal, and while individuals might have mnemonic preferences, access to the communicative potential of the Internet was not dependent on having a *specific* name – access only required that one had *a* name. Certainly, first-come, first served was not formulated with the explicit intent of preventing proprietary interests. However, precisely because it did not assign differential values to names, it reflected the general understanding of and the effort to maintain the Internet as an open and non-proprietary communicative space. Mueller therefore fails to account for the *normalization* of

propriety claims within the domain name space – in other words, he must answer how competition and property rights in the DNS became a 'fact' of Internet governance.

Drawing attention to the role of the *global marketplace* metaphor accounts for this normalization. While the combined effect of the World Wide Web and the privatization of the NSF backbone on their own certainly shifted the context of domain name use (and abuse), these changes occurred at the same time as the Internet was being championed as the frontier of the capitalist project to create a *global marketplace*. In other words, if the Internet itself had not been defined as *global marketplace*, the use of domain names for commercial purposes might have been possible but would not have had the same appeal. If people did not come to see the Internet as "shopping mall", there would not be a set of global consumers. Having a presence on the Internet would not be a business priority and domain names would not be lucrative real-estate. The definition of the Internet as a *global marketplace* accordingly had a catapulting effect: it did not just support the decision to allow the commercial use of use domain names but made domain names seminal and necessary instruments for successful global Internet commerce.

Some may argue that this redescription of the Internet by the *global marketplace* metaphor only accounts for creating a new realm in which businesses could compete for consumer marketshare. It does not explain how and why the domain name space itself became a global market. Mueller's account, in other words, holds – common pool resources are necessarily victim to property rights; the *global marketplace* metaphor only catalysed the inevitable. But this assumes that the two events – the domain name wars and the commercialization of the Internet – are unrelated. As the *Framework on Global Electronic Commerce* itself stated, once the Internet itself was a lucrative global marketplace, visibility

and competition in Internet-based commerce required specific rules and regulations about the use of domain names. On one level this had to do with ensuring that businesses could be competitive by preventing cybersquatting through effective trademark protection. On another, this had to do with the fact that if domain names could be linked to successful businesses, they were profitable real estate. The Internet's profitable potentials therefore extended to the 'value' of its name and number resources. To make the point very simply, the metaphor was consequential because the popularization of the Internet as a *global marketplace* redeployed the *communicative* capacities of the Internet as *commercial* ones. In so doing, domain names were necessary not only for accessing a communications medium but also for competing in a commercial marketplace. With their objective and purpose altered in this way, domain names were incorporated into the identity of a successful business entity. Once this happened, conflicts over property rights in the DNS were indeed inevitable: the *global marketplace* metaphor contributed to the rush for domain names because it legitimated the view that domain names could be property to which individuals and entities could claim exclusive rights, and that claiming such rights were essential for competing in the global economy.

How, then, does the *global marketplace* metaphor correspond to Mueller's description of ICANN as the product of a negotiated compromise between discordant interests driven by different strategic goals and desires for greater influence and power in domain name management and ownership? It does not dispute that ICANN was indeed an outcome of specific power plays and bargains between different actors. Attention to the metaphor simply illuminates the normative context in which such debates became possible in the first place.

As discussed above, the *global marketplace* metaphor legitimated not only the view that domain names were property but that they could be competitively bought and sold. In this way, it made competition the principal objective of DNS management. But the metaphor's influence extends beyond this. Its neoliberal premises linked effective competition to privatization. With respect to the technical community's privatization proposals, the metaphor's influence was subtle. The emphasis placed on privatization converged with the technical community's existing preference for keeping Internet governance in the hands of 'users'. What is evident is that the technical community largely did not contest that the Internet could be a global market. But, having accepted this, it contested how this commercialization should happen. A government monopoly in the DNS closed 'access', and therefore keeping it open required competition. The *global marketplace* metaphor's influence is therefore evident in the transformation the 'open access' into a vehicle for 'competition', which in turn reinforced the technical community's existing preferences for private authority in Internet governance. By contrast, the metaphor's neoliberal impulses directly informed the US government's privatization approach. Explicitly expressing its support for building the Internet as a *global marketplace*, the US government accepted that competition in this space required that it divest its role and promote privatization of the DNS space.

The ensuing debates that lead to the creation of ICANN were thus the outcome of this normative transformation of the Internet and its domain name space – promoting competition and requiring privatization. As the discussion in this chapter has shown, once actors converged around the *global marketplace* metaphor's vocabulary, their interests were redefined – the debate, as a result, was not over whether to privatize but how privatization

would occur. Thus the 'value added' by exploring the role of the metaphor in the debates resulted in the formation of ICANN is in how the emergence of the *global marketplace* as a way to describe the Internet normalized the view of the Internet as a commercial zone and reformulated domain names as property. Put differently, the metaphor reveals the emergence of a vocabulary that redefined the Internet's global space as an 'economy' in which domain names were 'scarce' and lucrative resources. In short, the metaphor illuminates not how ICANN was formed – i.e. the specific events and actors involved in putting it together – but why creating a competitive DNS space and privatizing the authority responsible for this task were *legitimated*.

The second argument against the influence of the *global marketplace* questions whether it actually displaced and disrupted logics of sovereignty in Internet governance. This argument is made in one of two ways. The first argues that while the metaphor did push in the direction of global governance, ICANN is ultimately the outcome of American hegemony. Although the US government argued that competition in the domain name space required the 'exit' of states, in the end, the US government decided the outcome. The US government rejected the IAHC and the ITU, and, despite deferring to the private sector to create a new private corporation, it made the final decision to endorse ICANN. The United States did effectively remove government influence in DNS management – i.e. by excluding the ITU and prohibiting governmental representation on ICANN's board – but it did so by 'locking in' its own sovereign preferences (c.f. Drezner, 2004, pp. 493-497; Mueller, 2002).

Yet, as Marlin-Bennett observes, "in the creation of ICANN, the United States government clearly indicated that it did not wish the International Telecommunications Union to be [the] source of governance. But neither did the US government take

responsibility for it itself" (qtd. by Drezner, 2004, pp. 495-496). From this perspective, ICANN is actually the outcome of the US government's attempt to remove all governments including itself from domain name management. It is indisputable that the United States had the authority to push forward privatization of DNS management: its legacy role gave it the exclusive power to even allow privatization. It is also clear that ICANN was an outcome of the US government's (and likely American business interests') preference for competition in the domain name space. But this is not on its own necessarily evidence of sovereignty – sovereignty, as argued, is a discourse that legitimates the state as the locus of political authority; it is not a synonym for it. Tracing the US government's use of the *global marketplace* metaphor reveals that even though the United States had a direct role in creating ICANN, it did so by promoting an alternative discourse of political legitimacy: rather than invoking sovereignty, it pushed forward the discourse of the 'self-governing' neoliberal market. So doing, it sought to entrench the understanding that *global competition* required relinquishing sovereignty. Thus, despite being the US government's preferred outcome, ICANN is not necessarily an expression of American *sovereign* power. The effort to create convergence around the Internet's global market potential and foster 'competition' meant that the process ultimately removed sovereignty – including that of the US – as the referent of political legitimacy.

Several commentators have argued that neoliberal globalization is a project of American imperialism – making the *global marketplace* metaphor a shorthand for a kind of US 'hyper-sovereignty.' Because of the US government's commitment to capitalism and the concentration of global business in the United States, promoting neoliberalism by attempting to inscribe the *global marketplace* metaphor as the normative framework of globalization

increases US power (Callinicos, 2005; N. Ferguson, 2004; Harvey, 2005b; Pieterse, 2004; N. Smith, 2005). Following this line of argument, ICANN is simply another example of America's emerging global empire – by creating ICANN over the ITU, the US government shut down opposition to neoliberal priorities. However, even a neoliberal *empire* dislodges the legitimating force of sovereignty. Aside from neoliberalism's disruption of sovereignty through competition, if it can be defined as a conventional empire, it would undermine the sovereign principle of non-interference. Imperial power, in other words, is the absolute abrogation of sovereignty. Thus, even if ICANN can be interpreted as a project of American empire, it would still be evidence of the normative disruption of sovereign governance.

Others, however, warn against attributing too much determinative power to the United States' role in promoting neoliberal globalization. While the United States has had a hegemonic (though not necessarily imperial) role in implementing neoliberal logics of globalization, "a time may be approaching when the institutionalization of globalization in various global forums might augur its continuation without domination by the U.S government" (Agnew, 2006a, p. 138) (c.f. Hardt & Negri, 2000; Hardt & Negri, 2004). The United States may have implemented the neoliberal *global marketplace* as policy orthodoxy. However, once taken as 'fact,' actors and institutions adhere to market principles on their own. Echoing Keohane (1984), adherence to neoliberal principles and practices by a variety of actors without coercion from more powerful actors is evidence that neoliberal globalization can continue 'after hegemony.' In the particular instance of ICANN, such appears to be the case once the *Framework for Global Electronic Commerce* and in time the Green Paper became the definitive reference texts for DNS privatization.

The second argument against ICANN as a manifestation of a global and non-sovereign political logic is that ICANN was the outcome of an inter-state bargain between the US and the European Union (Drezner, 2004, pp. 493-497). The key actors were states, not non-governmental agents. Drezner (2004, pp. 493-497) has argued that ICANN is evidence that 'global' governance outcomes are shaped by states. Deferring authority to a private organization was a state-directed outcome. Mueller (2002) further contends that the involvement of the US government and other key states means that ICANN is a "rough facsimile of an international treaty organization without a treaty." ICANN, in his perspective, represents the consolidation of state power over the root. Unlike Drezner who still interprets ICANN as a private agency, Mueller (2002, p. 211) asserts that despite all the privatization rhetoric, "the concept of 'privatization' … does not take us very far" when explaining ICANN

Both perspectives rightly demonstrate that global Internet governance does not by definition preclude the participation of states, as suggested in many cyberlibertarian accounts of Internet governance. However, in emphasizing the state, Drezner and Mueller suggest that the pressures of neoliberal globalization have had little impact on the state-centric structure of political order and authority. ICANN complicates this suggestion in two interrelated ways. First, ICANN negotiations took place among states as well as with a range of other actors. The US government's initial privatization policy was based on consultation with business groups. Magaziner's negotiations with IANA officials resulted in the conviction that IANA should be the foundation of the new corporation. While Postel consulted with different states to ensure support for his ICANN proposal, and required approval of the US government to take over the DNS management, the proposal itself was designed by non-state actors (i.e., the

technical community) (Mueller, 2002, pp. 177-184). In short, there was more to the ICANN story than an inter-state bargain between the US and the EU. Non-governmental actors had considerable influence in pushing forward certain objectives, such as trademark protection, privatization, and a central role for the technical community. Mueller (2002, p. 220) himself acknowledges that "ICANN is a product of a … bargain between the Internet technical hierarchy, a few major e-commerce and telecommunications firms, intellectual property interests (including WIPO), the European Union, and one or two other national governments."

Second, and perhaps more importantly, emphasizing the role of the state often neglects that a feature of neoliberal globalization is that private non-state actors are "accorded a form of legitimate authority" (Hall & Biersteker, 2002a, p. 4). ICANN is a vivid example of this. The dissemination of the *global marketplace* metaphor and the objective of competition legitimated the need for a private authority. This development did not, as Drezner and Mueller rightly note, remove states from the political landscape. But, with the normative focus on competition and neoliberalism, both of which contested the legitimacy of sovereignty, the landscape could not be reduced to states. At best, repeating a point made earlier in this chapter, once the neoliberal *global marketplace* became entrenched as policy orthodoxy, states became nodes in a new political complex and worked to implement policies that promoted global competition – in the case of ICANN, states advisory role in the GAC can perhaps be interpreted in this way.

Conclusion

In this chapter I have investigated how the *global marketplace* emerged as a discursive context for political order and how it then came to have an influence on Internet governance objectives, institutions and practices. Just as with the *global village* metaphor, the inscription of the *global marketplace* as a global governance framework relied on a convergence of changing socio-political conditions and specific developments that were already transforming the Internet. While the Internet's planetary reach made it a likely target for post-Cold War capitalist penchant to build a *global marketplace*, those efforts were facilitated by the development of the World Wide Web and the commercialization of the Internet.

I have argued that the desire to build the Internet as a *global marketplace* promoted a new vocabulary of *privatization*, *commercialization,* and *trademark protection,* which undermined the *state of nature* metaphor's social and economic welfare impulses and disrupted the assumption of the Internet as a public resource. This disruption pushed the globalization of the Internet in new directions by inscribing a new vocabulary of deterritorialization in which *territory* became effaced by the borderless market, which was embodied in the Internet, *population* came to signify a set of online global consumers, *authority* was placed in private institutions, and *recognition* was accorded to a global system of trademark law.

Although the exploitation of the Internet's global market potential took many forms, it was especially pronounced in the area of domain name management. As the Internet was popularized as a *global marketplace*, domain names became profitable commodities, generating questions about whether domain names could be bought and sold and by whom. The influence of sovereignty on Internet governance waned as the need for governments in determining policy for the domain name space was questioned. Though divided on several

issues, the technical community and the US government agreed on the idea of *competition* as the legitimating principle for developing the Internet's global commercial potential, with privatization and trademark protection as central objectives of DNS management.

I have shown that because the IAHC, spear-headed by the technical community, was unable to attend to the new interests in the user community and lacked the functional ability and policy authority to make changes to the Internet root, the debate about DNS management became focused on the provisions of the US government's *Framework for Global Electronic Commerce* and its Green and White Papers. These discussions resulted in a coalition supporting the US government's proposal for a new corporation and informally authorized Postel and IANA to take the initiative in determining the corporation's final structure. Once the US government endorsed their proposal for DNS management, DNS private authority was consolidated in ICANN. Because ICANN was given the task of creating and maintaining a global competitive market for domain names, its operational procedures – specifically, the GAC, the *UDRP*, and the limited participation of individual users – became ICANN's governance practices. Regular adherence to these practices reinforced the idea of the DNS as a global commercial space requiring competition and private governance, and helped to sanction the construction of the Internet as a *global marketplace*. Thus, if 'global' governance refers to the production of facts that define global space as a political order, then the *global marketplace* metaphor produced a form of Internet global governance by asserting competition as the 'why,' a global market for domain names as the 'what,' a private corporation (ICANN) as the 'where,' ICANN's board of directors and its commercial users as the 'who,' and the GAC, the *UDRP,* and the marginalization of individuals users as the 'how.'

Chapter 3

Global War on Terror: 'Global Security' and Internet Service Providers (ISPs)

Terrorists use the Internet just like everybody else
~ Richard Clarke, former White House cyber security chief

Introduction

On 5 July 2007, a British judge convicted Younis Tsouli of engaging in 'cyber jihad.' Tsouli was found guilty of using the Internet to propagate violent Islamic extremist ideologies and encourage others to carry out terrorist attacks. This case illustrates a growing recognition on the part of Western countries that the Internet is playing a seminal role in the orchestration of violent Islamic terrorist attacks and the radicalization and recruitment of their citizens to the jihadi cause. Recent policies to combat terrorism have therefore necessarily involved combating terrorist use of the Internet.

In the heightened security environment following the 9/11 attacks, the *global war on terror* has emerged as the latest description of globalization. Because of the importance accorded to the Internet in the growth of the terrorist threat, it has also developed as a discursive context for Internet governance. But, as a *war*, it has renewed the discourse on 'national security,' raising questions about the degree to which the phrase represents a continuation of *global* Internet governance. As 'security' is undoubtedly the metaphor's legitimating principle, the conventional approach has been to argue that it has ushered in a return to sovereignty, evidenced by increased state regulation of the Internet. However, in

this chapter, I will argue that precisely because this is a *global* war, the logic of security cannot be reduced to sovereignty. Rather, it oscillates between the conventional approach to protecting state sovereignty and the recognition that because the nature and location of threats and enemies have fundamentally changed, new approaches to security are required. The *global war on terror* metaphor therefore inscribes complex and contradictory governance logics. But despite the emphasis on 'national' security, there are pressures and normative principles that are pushing forward the Internet's global governance.

To illustrate the inscription of the *global war on terror* metaphor, I examine how political leaders, policy makers, law enforcement, and intelligence agencies have established the metaphor as a new vocabulary for Internet governance in the United States, United Kingdom, and by the Council of Europe in its Convention on Cybercrime. Because countries such as the United States, the United Kingdom and others in Europe have been acutely affected by terrorist attacks, discussions of *global war on terror* are particularly prominent in these contexts. They therefore illustrate the effects of the *global war on terror* as a metaphor for Internet governance, (c.f. Lyon, 2003), although their specific approaches to terrorism differ from those in other parts of the world

It is important to acknowledge that the *global war on terror* has not become *the* hegemonic framework of global Internet governance. It is limited to discussions of the security implications of the Internet as they relate to anxieties about terrorism. But given ways in which this metaphor has occupied and assumed a prominent place in the collective political imagination, and they way the fight against terrorism has been linked to the Internet, how this most recent metaphor of globalization is creating new developments in Internet governance is worth exploring.

I contend that the consequence of the turn towards the *global war on terror* as a metaphor for Internet governance has been the development of new state powers for Internet surveillance and censorship that place new responsibilities on Internet Service Providers (ISPs). With attention directed to how terrorism has proliferated through use of the Internet, ISPs have been considered indispensable in fighting the terrorist threat. As the vocabulary of the *global war on terror* becomes entrenched, ISPs and their surveillance and censorship practices are emerging as governance mechanisms of greater state control but within a new *global* governance effort.

Globalization, the *global war on terror,* and the Internet

Presenting the *global war on terror* as a metaphor of globalization is contentious. Even a cursory examination of counter-terrorism efforts in the United States and the United Kingdom, amongst other Western countries, demonstrates that despite references to a 'global' war following the 11 September 2001 attacks, the focus has been on 'national' or 'homeland' security. Although governments around the world have acknowledged that the enemy can no longer be identified as another state but instead as Islamic extremist terrorist networks with "global reach," the attack has been articulated as one on the state (U.S. Government, 2002, p. 5). In the US, for instance, counter-terrorism policies emphasize that the objective is to 'Protect America.'[82] In light of these developments, a number of commentators have suggested that the *global war on terror* might not be a metaphor of *globalization* but instead might signal the 'end of globalization' and a return to sovereignty (Acharya, 2007; Gray, 2002; Hobson, 2007; Robert Jackson, 2007; Troyer, 2002).

[82] See for instance the Protect America Act of 2007.

A discourse that puts emphasis on territorial borders as the markers of political authority, sovereignty's (renewed) importance can be discerned through the urgency given to border protection. With a consensus that "strong borders" are "essential" to protect against terrorism, governments worldwide have tried to enhance security with new surveillance technologies, visa regulations, and other forms of border control (Cabinet Office, 2008, p. 57) (c.f. Amoore, 2007; Andreas, 2003; Lyon, 2003; Moran, 2005; Sparke, 2006).

Jackson (2007) argues that security can be provided by states *only*. This view privileges sovereignty's definition of security as the defence of territorial borders – the protection of 'insiders' (citizens) from 'outsiders' (foreigners) – and thereby the exclusive and even foremost responsibility of states (Dalby, 1992; Walker, 1993, 1997). Consequently, even though the terrorist threat is acknowledged as differing from aggression by rival states (and therefore the 'dilemmas' of the *state of nature*), securing against it requires a return to the political legitimacy of sovereignty and state authority (Bajc, 2007, p. 1580).

The more profound implication of this position is that security requires protecting the ontological status of the state and the states-system as the appropriate structure of political authority – otherwise, the world will remain susceptible to terrorist threats. According to Acharya (2007, p. 275), this line of reasoning is why the war on terror "has been framed overwhelmingly as [an existential] threat to security and *international* order" (my emphasis). As Douglas Feith, former US Undersecretary of Defense for Policy, stated:

> The United States strengthens its national security when it promotes a well ordered world of sovereign states … The importance of promoting a well-ordered world of sovereign states was brought home to Americans by 9/11, when terrorists enjoying safe haven in remote Afghanistan exploited 'globalization' and the free and open nature of various Western countries to attack us disastrously here at home. Sovereignty means not just a country's right to command respect for its independence, but also the duty to take responsibility for what occurs on one's territory, and, in particular, to do what it takes to prevent one's territory from being used as a base for attacks against others. (qtd. in 2007, p. 279)

Understanding the war on terror in these terms has led the US and other like-minded governments to assert that "today, the world's great powers find ourselves on the same side – united by the common dangers of terrorist violence and chaos" (U.S. Government, 2002). With the security of the states-system itself at stake, they have also promoted a responsibility to intervene and bolster the sovereignty of 'failed' states (Cabinet Office, 2008; U.S. Government, 2002). Protecting sovereignty as the principle of political rule has thus become essential in securing against transnational terrorism.

Unlike the 'borderless' global orders promoted by the *global village* and *global marketplace* metaphors, the effort to combat 'global' terrorism appears – perhaps ironically – to have sanctioned territoriality rather than principles of 'global' governance. In light of initiatives to enhance the protection of *territorial* borders, the *populations* they circumscribe, the *authority* of states, and, as Feith emphasized, to ensure that sovereignty is the basis of political *recognition*, the *global war on terror* metaphor appears to reinforce the normative purchase of sovereignty.

But to suggest that the security efforts associated with the global war on terrorism indicate a return to sovereignty is a limited interpretation. Although the 2002 US National Security Strategy states that "Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government," it also contends that "today that task has changed dramatically. Enemies in the past needed great armies … to endanger America. Now shadowy networks of individuals can bring great chaos and suffering to our shores" (U.S. Government, 2002, p. 5). Likewise, in the lead up to the UK's 2008 National Security Strategy, Prime Minister Gordon Brown (2008) claimed that the "obligation to protect the British people and the national interest is fixed and unwavering" but that "the nature of the

threats and risks we face have … changed beyond recognition and confound all the old assumptions about national defence and international security … New threats demand new approaches". Reterritorializing policies evidently invoke a deterritorialized notion of security. Observing this trend, Sparke (2006, pp. 152-153) argues that it is necessary to "move beyond the anachronistic methodological nationalism of arguments that posit the protection of … citizens and the defense of national borders as two defining features of … state-making." Instead, it is necessary to attend to the *global war on terror*'s complex and contradictory consequences for political order.

These complex and contradictory implications, according to Barkawi (2006, p. 131), result from the fact that "while [the global war on terror] is fought in and through a world of states, many of the terms are not reducible to nation-states." The most obvious instance of this is the articulation of the war as a "global enterprise" against "shadowy networks of individuals" (U.S. Government, 2002, p. 5) (c.f. Deibert & Stein, 2003). However, globalizing the war has only partly been a result of terrorist networks' ability to cross territorial boundaries. What is more significant is how this has resulted in the normative reformulation of the referents of war and security beyond sovereignty.

Such reformulation can clearly be seen in the shifting definition of the enemy. Although the enemy was initially defined as 'soldiers' deployed by corporate al-Qaeda, the growing worldwide radicalization of young Muslims has shifted attention to the threat posed by individuals who join the terrorist effort with no explicit connection to al-Qaeda other than a desire to emulate its methods and carry out its call for 'global jihad' (Brachman, 2006; Conway, 2002; R. Katz & Devon, 2007; Kohlman, 2006b; Raban, 2005). Consequently, government policies have acknowledged that the current threat is unlikely to be lodged by

another state or even a single organization, "but a wider network of affiliated groups, often sharing a common ideology and outlook" (Cabinet Office, 2008, p. 11). The enemy has therefore been identified as a 'global Islamic insurgency,' 'global Islamo-fascism' or 'violent Islamic extremism' (Barkawi, 2006; Gordon Brown, 2007; Macdonald, 2007; A. Russell, 2005).[83]

The effects of worldwide radicalization have also revealed a new kind of 'homegrown terrorism' – the radicalization of young Muslim citizens, usually in Western countries. Rather than assuming that terrorists are only foreign nationals who infiltrate a country with the intent to inflict harm on its civilian population,[84] states have come to see the citizen too as a would-be terrorist. With citizens *and* foreigners as possible 'enemy combatants,' the global scope of the enemy is no longer simply a matter of a foreigner's ability to cross borders and infiltrate a targeted state. Rather, borders become irrelevant references for distinguishing between 'friends' and 'enemies' and identifying sources of threat. According to Mitchell Silber, Senior Intelligence Analyst for the NYPD, "while the threat from overseas remains, most of the terrorist attacks or thwarted plots against cities in the West since 9/11 have fit a different pattern. The individuals who plotted or conducted the attacks were generally citizens or residents of the nations in which the attacks occurred" (qtd. in United States Senate Committee on Homeland Security and Governmental Affairs, 2008, p. 2).

Understanding threat and enemy in these terms has had a concomitant effect on who or what is to be defended or secured. Early on, President Bush asserted that the 'war on

[83] Beginning in 2005, there was an effort, especially by the US and UK governments to move away from the 'global war on terror' and articulate the conflict as a struggle against 'Islamo-fascism' or 'Islamic extremism.' Moving away from explicit mention of the metaphor does not mean that it has been abandoned. The definition of the enemy as 'Islamo-fascism' or 'Islamic extremism' suggests that it remains the primary discursive context for anti-terrorism strategies (c.f. Macdonald, 2007; A. Russell, 2005; Travis, 2008)

[84] This assumption was based on the experience of the 9/11 attacks, carried out by foreign nationals. The assumption received more formal articulation in the immediate aftermath of the attacks when then US Attorney General John Ashcroft established the 'Foreign Terrorist Tracking Force.'

terror' is not "just America's fight … This is civilization's fight" (G. W. Bush, 2001a). British Prime Minister Tony Blair reiterated this view following the 7 July 2005 London bombings, stating that the attacks were an affront to "all civilised people" (Blair, 2005). Although the *global war on terror* has also been envisioned as a conflict between states – states who harbour terrorists can be targets of war because the "allies of terror are the enemies of civilization" (U.S. Government, 2002, p. 5) – when framed in the context of the fight against global terrorism such interstate conflicts are not operations of sovereignty as such but situated in a broader conflict between 'global terror' and 'global civilization.'

If the networked structure of global terrorism has redefined the identity of the enemy and the population to be protected, it has also resituated security efforts. Because the enemy is not limited to a particular state, officials find it unlikely that the war on terror will be fought on "battlefields and beach-heads" (Dam qtd. in Richard Jackson, 2005: 148). Instead the "global reach" of terror networks means that "the struggle against global terrorism … will be fought on many fronts against a particular elusive enemy" (U.S. Government, 2002, p. 5). While protecting borders remains important for preventing the entry of foreigners with harmful intentions, and campaigns abroad, such as in Afghanistan, possibly to prevent the capture of states by terrorist groups, they are not sufficient responses. 'Homegrown terrorism' makes the domestic sphere an equally important battleground. As UK Prime Minister Gordon Brown (2007) put it: the war on terror will be fought "at home and abroad."

These reformulations clearly demonstrate the deterritorializing vocabulary of 'global' security that accompanies the reterritorializing discourses and practices of 'national' security. In light of a new kind of enemy and threat, conventional *territorial* referents of war – battlefields and beachheads – are giving way to networks, with the subsequent need to fight

the war 'at home and abroad.' The definition of *population* no longer makes a clear distinction between 'citizens' and 'foreigners' but instead differentiates 'global civilization' and 'global terrorist networks.' This raises questions about exclusively defining states' *authority* in the terminology of sovereignty. Although sovereignty is recognized as an important principle, those states considered terrorist 'allies' or susceptible to terrorist capture are not accorded the rights of *recognition* established by *de jure* norms of sovereignty. It would therefore seem that the vocabulary of the *global war on terror* metaphor, while putting a premium on 'national' security, also inspires a security effort that cannot be reduced to sovereignty.

Evidently, the *global war on terror* has had a far more paradoxical effect on sovereignty than initial readings of state action would suggest. Acharya (2007, p. 275) perhaps captures it best: "the war on terror is justified as protecting 'national security' from a transnational menace which challenges it by its very mode of organisation and operation and its presumed political agenda, … But in so doing, the leading state [the United States] waging this war and its supporters also exempt themselves from the norms of the Westphalian order, and approve instruments that could be profoundly subversive of that order." This is more than 'organized hypocrisy' (Krasner, 1999). The normative redefinition of war by states lends support to Sassen's claim that the denationalizing effects of globalization often lie deep within the actions and initiatives of the state itself. This accounts for the prominent role of the state in the war on terror. But it also calls our attention to how protecting 'national' security against a new kind of threat not only fortifies sovereignty but also contributes to the globalization of political order under a 'global' security principle (c.f. Beck, 2005, pp. 88-89; Held & McGrew, 2007; Kaldor, 2006).

Tying the Internet to the anti-terrorism effort has been triggered by evidence that the Internet was used to orchestrate the 9/11 attacks and has played a key role in the radicalization of young Muslims. Use of the Internet for malicious purposes has been a long-standing concern for policy-makers. However, until the 9/11 attacks, and later those in London, Internet legislation was largely focused on financial fraud schemes by organized crime groups, copyright infringements, and child pornography. Lawmakers have now added terrorism to the Internet governance agenda.

To combat the 'online' terrorist threat, governments around the world have expanded their powers of surveillance and censorship (Lyon, 2003). This trend may not be surprising in democratically challenged states, with longstanding Internet surveillance and censorship policies. However, terrorist use of the Internet has intensified efforts in liberal democratic countries, such as the United States and the United Kingdom, to exert greater control over cyberspace (Deibert, Palfrey, Rohonzinski, & Zittrain, 2008; Lyon, 2003).

Interpreting these expanded state powers as a consolidation of sovereignty as the legitimating principle of Internet governance, commentators have argued that surveillance and censorship, driven by national security, have 'territorialized' the Internet, undermining the open, borderless communications and commerce envisioned by cyberlibertarians and those who view the Internet as a *global marketplace*. In other words, concerns about national security associated with the *global war on terror* invoke a need for 'border control' on the Internet and potentially reverse the Internet's globalization (Goldsmith & Wu, 2006) (c.f. Deibert, Palfrey, Rohonzinski, & Zittrain, 2008).

Yet, as stated above, the *global war on terror* metaphor is fraught with normative tensions between the desire to protect national security (reterritorialization) and the

emergence of a less discernable enemy and threat (deterritorialization). This tension is especially acute in the realm of Internet governance. Not only does the technical architecture of the Internet evade borders, but use of the technology by terrorists disperses the enemy among many different locations. Conventional attempts to protect borders are therefore ill-suited for addressing terrorist use of the Internet (c.f. Krishna-Hensel, 2007, p. xi). Evidently, while sovereignty has influenced the objectives of Internet governance, the *global war on terror* metaphor also creates pressures that foster the Internet's globalization.

In the remainder of this chapter, I explore how the *global war on terror* metaphor pulls the Internet (back) into the realm of 'national' security but also inscribes vocabularies that continue its globalization. As stated, my analysis focuses on anti-terrorism efforts in the United States and the United Kingdom and the Council of Europe's initiatives on cybercrime and the new roles these have created for ISPs. To reiterate, Internet surveillance and censorship are not new practices in democratic and non-democratic countries alike. I will demonstrate that the normative tenor of the *global war on terror* metaphor has uniquely defined and directed them in a continuing, if at times contradictory, pattern of global governance.

Legitimacy crisis: calling into question the sovereign security effort

As the responsibility for fighting terrorism has traditionally fallen to the state, governments have responded to terrorist use of the Internet by expanding their participation in Internet governance. This marks a notable change from the developments noted in the previous two chapters, in which the legitimating force of the *global village* and *global marketplace* shifted

aspects of Internet regulation away from governmental authority to users and/or private regulators. Since it falls under the rubric of national security, this 'return to the state' would seemingly entail a return to sovereignty. However, terrorist use of the Internet, while prompting security concerns and greater action by governments, has also raised challenges that complicate the ability and desire of governments to inscribe sovereignty as the legitimating context of Internet governance.

At first, concerns about terrorist Internet use involved the possibility of 'cyberterrorism' – the use of computer networks to carry out attacks on 'critical infrastructures,' such as public utility grids, emergency services switchboards, or computer networks themselves (Bendrath, 2003; Colarik, 2006; Denning, 2000, 2001). In light of the 1993 World Trade Centre bombing, the 1998 attack on the US embassy in Kenya, and the attack on the USS. Cole in 2000, attention to asymmetrical warfare highlighted how the Internet provided a cheap and easily employable means of waging war. Following the 9/11 attacks, the possibility of a cyber-enabled terrorist attack became an overriding concern.

Although a number of officials, especially in the US, were aware that al-Qaeda was using the Web to organize its network and recruit new members, this kind of use of the Internet remained a secondary concern until the Taliban was ousted from power in Afghanistan. Brachman (2006) argues that in the absence of a state sponsor, al-Qaeda leaders elected to make more strategic use of the Internet to keep the network from fracturing. Developing sophisticated jihadi websites, the al-Qaeda leadership exploited the Internet's communicative potential to spread its "ideology [and] its know how through documents [and] through videos" (c.f. I. Black, 2008; Kohlman, 2006a, 2006b).

Al-Qaeda's move to cyberspace, however, had a somewhat unexpected effect on the overall morphology of jihadi movement. Because "every machine on the Internet is potentially a printing press, a broadcasting station, or place of assembly," al-Qaeda's ideological message is no longer espoused only by its leadership or formally connected members (Conway, 2002, p. 436). Rather, the Internet provides a free platform for sympathetic individuals to vocalize their support or find likeminded others with whom they can collaborate to launch an attack – all without the formal support or knowledge of al-Qaeda 'central' (Sageman, 2008). Effective use of the Internet – through websites and chatrooms – has therefore transformed the al-Qaeda terrorist threat from an interconnected web of cells with a central point of control to a "decentralized, transnational patchwork of terrorist cells that no longer relies on al-Qaeda to mobilize and carry out attacks" (R. Katz & Devon, 2007). Consequently, although efforts to prevent cyber-enabled attacks continue,[85] a greater priority is placed on preventing the proliferation of a dispersed, informally organized planetary network of radicalized individuals and their appropriation of the Internet's communicative power (Conway, 2007, p. 25).

Use of the Internet to promote violence is a significant departure from the peaceful dialogue envisioned by proponents of the *global village* metaphor. Ironically, the Internet's open communications system has enabled Islamic terrorists to flourish as a threat beyond al-Qaeda. Furthermore, terrorists have exploited the commercial dimensions of the Internet

[85] In the United States, concerns about cyberterrorism prompted the creation of a National Strategy to Secure Cyberspace. Specific protection against cyberattacks were also legislated in Section 8 of the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' Act (USA PATRIOCT Act). The British government has made similar provisions with the creation the Centre for the Protection of National Critical Infrastructure in 2001. Protecting critical infrastructures was also listed as a priority in its 2008 National Security Strategy. Protection of National Critical Infrastructure in 2001. Protecting critical infrastructures was also listed as a priority in its 2008 National Security Strategy. Protection of National Critical Infrastructure in 2001. Protecting critical infrastructures was also listed as a priority in its 2008 National Security Strategy.

established by the *global marketplace* metaphor by financing their efforts with such things as credit card fraud schemes (Conway, 2006, pp. 285-286).

The security concerns raised by terrorist (mis)appropriation of the peaceful and profitable potentials of the Internet for more pernicious ends have prompted a state response. Greater state control contests the cyberlibertarian principles associated with the *global village* metaphor and compromises the Internet's capacity to foster free expression and dialogue (Barlow, 1996; Godwin, 2003). Commercial interests might also find sovereignty's protective 'bordering' logic a prohibitive factor for enhancing the electronic *global marketplace*, although combating terrorism might also create a more stable environment for commerce.

Yet while state control seems a far departure from the governance agendas and frameworks of the *global village* and *global marketplace* metaphors, there has not been an automatic reversion to sovereignty. Terrorist use of the Internet has challenged conventional understandings of and approaches to national security, and has created incentives for continuing the global governance of the Internet, albeit with different objectives.

The pressures for global governance are both functional and normative. Functionally, if terrorists use the Internet to organize and orchestrate attacks, governments must be able to track Internet communications. However, such communications can hop from country to country, even if the final destination is within the same country. Because states accordingly need the capacity to monitor communications as they travel through other jurisdictions, there is an incentive for states to abandon some sovereignty – by allowing each other to monitor what goes on 'inside' their respective territories, they may collectively be able to avert a potential attack against any or all of them. A normative commitment to sovereignty, in other

words, may inhibit the detection of terrorist networks and compromise national security. Sovereignty's 'legitimacy crisis' therefore rests in the paradox that protecting national security may require partially abandoning sovereignty – strictly abiding by it may not be the most efficacious response to the growing terrorist threat.

Incorporating the political vocabulary of 'global security'

With growing awareness that the Internet's threat potential rests not only in the possibility of cyberattacks but also in being used to organize and recruit new members to Islamic extremism, Latham (2003, p. 2) argues that the *global war on terror* has been a "pivotal [and] important moment to redefine missions and approaches" with respect to Internet governance. In this section, I trace the incorporation of the *global war on terror's* vocabulary into Internet governance policy by the US and UK governments and the Council of Europe – specifically delineating how legislators define the Internet as a 'front' in the war on terror. Although this effort is inspired by concerns about sovereignty, articulated through the rubric of 'national' security, the Internet's role in creating a dispersed enemy that confounds distinctions between 'citizens' and 'foreigners' is developing a more complex set of facts that, while defining governance objectives towards sovereignty, also promote principles of global Internet governance.

In the weeks following the 11 September 2001 (9/11) attacks, FBI Assistant Director Ronald Dick testified that the hijackers had used the Internet and "used it well" (qtd. Conway, 2002). Investigations revealed that the attackers had bought their airline tickets online and formulated and shared the operational details of the attack using email, sometimes

using terminals in American public libraries. In light of this, the Department of Justice sought to update surveillance laws to meet the specific technical features of Internet-based communications. Although pressures to do so pre-existed the terrorist attacks, the hijackers' use of the Internet made the effort more urgent. 9/11 became an opportunity to usher in desired changes to Internet surveillance laws to "assist law enforcement in terrorism related cases" (Kerr, 2003, p. 636).

This update has been accomplished most visibly through the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* ('PATRIOT' Act), passed immediately following the 9/11 attacks in October 2001. The PATRIOT Act has been the most extensive piece of anti-terrorism law in the United States as well as the first substantive legislation on the Internet in fighting terrorism. As then US Attorney General John Ashcroft (2001) put it, with the passing of the PATRIOT ACT, "investigators will be directed to pursue aggressively terrorists on the internet." Since then a number of legislative efforts have reinforced the importance of the Internet in anti-terrorism.[86] However, as the initial response to terrorist use of the Internet, the PATRIOT Act is an illuminating reference point for understanding the effect the *global war on terror* metaphor has had on US Internet governance policies.

The PATRIOT Act describes the Internet as a front in the fight against global terrorism by explicitly modifying the language of surveillance laws to enable Internet surveillance (Bellia, 2003; Dean, 2003; Kerr, 2003; Solove, 2003). Pen registers[87] have been

[86] See for instance the *Violent Radicalization and Homegrown Terrorism Act* (awaiting Senate approval), the Electronic Surveillance Modernization Act (awaiting Senate approval), and the Protect America Act (signed into law 17 February 2008). Changes have also been implemented through an update or revision of existing laws, for example, the 2004 amendments to the Communications Assistance for Law Enforcement Act.

[87] Pen registers originally referred to electronic devices that recorded all phone numbers dialled from a particular telephone line. It is now understood to be any electronic device that performs similar functions, for instance, those that monitor Internet communications.

updated to include not just "dialing" but "routing, addressing or signaling information" (Section 216(a)). In addition to access to customer name, address, phone numbers, billing records, and the list of services used, law enforcement can now obtain "records of session times and durations," "any temporary assigned network address," and stored emails (Section 210). Although serving a number of objectives, the Act's introduction of nationwide search warrants has in part been motivated by the 'real time' character of Internet communications, making it easier to trace the path of an email message. Such changes have not simply updated electronic surveillance laws so that they apply to the Internet. Legislated as part of the US government's strategy to combat global terrorism, legalizing email headers, IP addresses, and URLs as objects of surveillance has enrolled the Internet in the new security environment associated with the war on terror (c.f. Deibert, 2003). While several of the PATRIOT Act's Internet surveillance measures were subject to a sunset clause, when the Act was renewed in 2005, the Department of Justice argued that these capacities had been so important in the government's anti-terrorism efforts that failure to renew them would result in a reversion to a "pre-9/11 mode of information … where the terrorists can use the technology against us" (qtd. in Jones, 2005). So when the Act was reauthorized, its Internet surveillance provisions were also renewed.

The terminology of the Act's mission as 'United and Strengthening America' illustrates how the new security environment for the Internet is informed by the objectives of 'national' security – albeit in a somewhat redefined form. This is most obvious in the priority placed on 'foreign' terrorists as sources of enemy threat (Section 411). Of course, rival states can still be menacing and endanger national security (as the 'axis of evil' and 'rogue' states discourse demonstrates). Based on the experience of the 9/11 attacks, however, a key

national security concern has revolved around how foreigners infiltrate the United States in order to conduct terrorist attacks on the civilian population, hence the Act's provisions for enhanced border control and new immigration restrictions (Sections 401-428). Although at the Act's passing, terrorists were considered to be those with connections to recognized terrorist organizations, principally al-Qaeda, the arrest of Zacarias Moussaoui drew attention to individuals inspired by al-Qaeda's message to take their own initiative to fight the jihad. The Moussaoui Fix Bill, passed in 2003, expanded the definition of the foreign terrorist to include 'lone wolf' terrorists.[88] As the co-sponsor of the Bill, Senator Charles E. Schumer, stated: "we live in a world where the greatest threats to our freedoms can come from the person acting on his own … By passing this bill we are sending a message to all terrorists: if you're not an American citizen, you don't have a green card, and we have reason to believe that you're plotting terrorism, the FBI will be watching you."[89] In these formulations, the definition of the enemy, while evolving from an exclusive focus on rival states, still employs the discourse of 'foreignness,' suggesting that the terrorist is always a non-national, 'external' threat. Internet surveillance has therefore been geared toward identifying the 'foreigner' lurking within, who may be using the Internet to plan an attack. To this end, electronic surveillance law has also eliminated restrictions on information sharing between

[88] Section 101: Individual Terrorists as Foreign Powers. Under 50 USC. § 1801(a)(4), the definition of "foreign power" includes groups that engage in international terrorism, but does not reach unaffiliated individuals who do so. As a result, investigations of "lone wolf" terrorists or "sleeper cells" may not be authorized under FISA. Such investigations therefore must proceed under the stricter standards and shorter time periods set forth in Title III, potentially resulting in unnecessary and dangerous delays and greater administrative burden. This provision would expand FISA's [Foreign Intelligence Surveillance Act] definition of "foreign power" to include all persons, regardless of whether they are affiliated with an international terrorist group, who engage in international terrorism (http://www.talkleft.com/story/2003/05/08/952/90859) [21 November 2007]

[89] http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/PR01681.html

law enforcement and intelligence agencies so that the foreign terrorists lurking within the national space can be identified.[90]

The 7 July 2005 (7/7) bombings in London reinforced fears that the Internet could be instrumental in the planning and preparation of a terrorist attack. As one commentator put it, "The London attacks were a modest, simple affair carried out by four seemingly normal men using the Internet" (qtd. in Townsend, 2006). However, 7/7 created a problem: foreign nationals who entered the UK did not carry out the attacks – they were planned and executed by *British* citizens. Domestic sources of terrorism are not a new development in the UK. Up until the late 1990s, the UK's experience with terrorism was largely defined by its experience with the Irish Republican Army (IRA). However, following the emergence of al-Qaeda, the 2000 Terrorism Act updated the definition to include 'international' terrorist groups. Based on al-Qaeda's role in the 9/11 attacks, the 2001 Anti-Terrorism, Crime and Security Act reinforced the focus on international terror groups. As the Home Office stated in its defence of the Act, "the attacks in New York and Washington on September 11 represent an escalation in the scale and scope of the international terrorist threat to our interests … Through improved protection, tracking and prevention of terrorism, the Government considers that the Bill will contribute to an improved level of security for the UK, preventing loss of life and ensuring that businesses and society as a whole continue to operate in safety" (qtd. in Saliban and Sykes 2002: 338).

Although the Act acknowledged that international terrorists operated in transnational networks that could function within British society, like the PATRIOT Act, they were understood to be foreign nationals who had links with groups such as al-Qaeda. As a result,

[90] This has been instituted by the Act's amendments to the 1978 Foreign Intelligence Surveillance Act, which put tight restrictions on the executive's power to conduct domestic surveillance, especially on US citizens.

the Anti-terrorism, Crime and Security Act's strategy similarly revolved around border control, and new regulations for immigration, asylum, and deportation (Part 4, Sections 21-32). To the extent that the Internet was considered important in anti-terrorism strategies, the Anti-Terrorism, Crime and Security Act redirected the UK's existing surveillance laws. In the event of a terrorist attack, the Act's supporters hoped that various data retention requirements would allow law enforcement and intelligence agencies to trace communications that could potentially reveal the identity of terrorist attackers and/or find evidence of plots that could be used to prosecute suspected terrorists.

The 7/7 attacks interrupted the presumed 'foreignness' of terrorist attacks by bringing to light the growing trend of 'homegrown terrorism' (Intelligence and Security Committee 2006). Although the initial impulse was to find a link between the bombers and al-Qaeda, it was soon clear that such an assumption was untenable. As one police source put it, "All the talk about … al-Qa'ida masterminds looks like something from a film script … It looks increasingly as if these were people acting on their own" (qtd. Bennetto & Herbert, 2005). In other words, the London bombers were a *self-started* terrorist cell (Kirby, 2007). Evidence that this trend is growing has led Prime Minister Brown (2008) to redefine the terrorist threat as coming "from *loosely affiliated global networks* that threaten us and other nations across continents" (my emphasis).

Homegrown terrorism has drawn specific attention to the role of the Internet in radicalizing citizens and morphing the threat from violent Islamic extremism beyond any concrete association with al-Qaeda. In the immediate aftermath of the of the London bombings, attention turned immediately to the Internet. British Prime Minister Tony Blair (2005) argued that it was necessary to "look at their websites" to understand how al-Qaeda

was spreading an "evil ideology" that was recruiting young British Muslims as "fellow travellers" in a "global struggle." The UK Home Secretary at the time, Charles Clark (2005: col. 1254), announced that the state would be expanding its power to "deal with those who foment terrorism or seek to provide others to commit terrorist acts" by targeting those "preaching, running websites or writing articles intended to foment or provoke terrorism."

If such proclamations were in part reactionary and based on conjecture, they received confirmation by government working groups tasked with developing strategies for preventing the radicalization of British youth. Its final report, entitled *Working Together to Prevent Violent Extremism* (2005), noted that "much learning about Islam is autodidactic – rather than being based on teachings in the mosque, for example. This has resulted in innovation and creativity but has also provided opportunities for the propagation of extremist ideology" (p. 18). As part of this trend, it claimed that "an increasing number of young Muslims are turning to the Internet for information on Islam" (p. 94) With the number of extremist sites outnumbering mainstream Muslim websites, the Internet was taking a central role in the radicalization of Muslim youth in the UK (c.f. , p. 94).

In the 2006 Terrorism Act, a response to this new Internet-driven homegrown terrorism, the Blair government defined new crimes related to inciting, justifying, or glorifying terrorism and applied them directly to the distribution and consumption of material and messages circulated on the Internet (Part 1, Section 3). The incumbent Brown government has bolstered this effort. Announcing a new anti-terrorism strategy in December 2007, Brown stipulated that eliminating "extremist influences operating on the Internet" would be a continuing government priority. Current UK Home Secretary, Jacqui Smith, has reinforced this objective, arguing that it is necessary to take steps "to show that the Internet is

a no go area" for terrorists (qtd. in Mulholland, 2008). That terrorist use of the Internet has become part of the UK's government's national security vocabulary is apparent in the 2008 UK National Security Strategy. The 'new terrorist threat', it claims, "[exploits] modern travel and communications (especially the Internet) to share information, personnel and training, and to spread a common ideology – working together in ways that were not possible for terrorist groups in the past" (Section 3.7).

The US government has similarly laid blame on the Internet for fostering homegrown terrorism. On 24 October 2007, the House of Representatives passed the *Violent Radicalization and Homegrown Terrorism Act*, in which the Internet was singled out as "facilitating violent radicalization, ideologically based violence, and the homegrown terrorism process in the United States by providing access to broad and constant streams of terrorist related propaganda to United States citizens" (Section 899B (3)).

This view is echoed in a recent report by the US Senate Committee on Homeland Security and Governmental Affairs, entitled *Violent Islamic Extremism, the Internet and the Homegrown Terrorist Threat* (2008). Based on the testimony of top US law enforcement and intelligence officials, the Report (2008, p. 15) concludes that "the use of the Internet by Al Qaeda and other violent extremist groups has added new dimensions to the terrorist threat faced by the United States. No longer is the threat just from abroad, as was the case with the attacks of September 11, 2001; the threat is now increasingly from within, from homegrown terrorists who are inspired by violent Islamic ideology to plan and execute attacks where they live."

US lawmakers and their UK counter-parts have been careful not to put the full responsibility for homegrown terrorism on the Internet. The preconditions for radicalization

likely rest in a sense of marginalization among Western Muslims and/or anger about Western foreign policies, particularly relating to the war in Iraq (Sageman, 2008; United States Senate Committee on Homeland Security and Governmental Affairs, 2008, p. 4; Working Group on Preventing Violent Extremism, 2005).[91] At best, the Internet provides a platform for those who are already jihadi sympathizers. Its advanced communications structure, however, hastens the trend by replacing the need to travel to training camps in Afghanistan for indoctrination in violent Islamic ideology and training in jihadi methods: radicalization can happen online (United States Senate Committee on Homeland Security and Governmental Affairs, 2008). Charles E. Allen (2008), Chief Intelligence Office at the Department of Homeland Security, argues that in the past year al-Qaeda and like-minded groups have "ratcheted up the speed and accuracy of translated statements openly marketed to US and English-speaking audiences" and that "several radical websites in the United States have re-packaged al Qaeda statements with American vernacular and comments intending to sway US Muslims."

Although the US government has not yet taken formal action to combat homegrown terrorism in a manner similar to the UK's 2006 Terrorism Act, it has acted in other ways. Most prominently, the concern that US citizens, rather than just foreign nationals, are joining terror networks appears to have been the motivation for the President's authorization of the National Security Agency's (NSA) secret domestic surveillance program (Risen & Lichtblau,

[91] Sageman (2008) notes that the risk of radicalization in the United States is far less than in European countries because of the relatively high rate of successful integration of Muslims into American society. The Senate Committee's Report on *Violent Islamist Extremism, the Internet and Homegrown Terrorism* (2008, p. 4) makes a similar argument, asserting "that [the radicalization] process has been less likely to occur in the United States than in other countries. Some attribute this to the unique cultural influence of the "American experience" and the general absence of a sympathetic audience in the United States. For the most part, America's diverse Muslim communities are well integrated into our society and want to raise their families in safe and peaceful communities. And unlike some countries in Europe and elsewhere, the 'longstanding tradition of absorbing varied diaspora populations has protected the United States and retarded the radicalization process at home.'"

2005).[92] President Bush (2006) has reiterated that surveillance has been conducted only on those US citizens thought to have a connection with a *foreigner* who is a target of a US terrorism investigation, and has therefore monitored only their *international* telephone and Internet communications. While the focus is still on 'foreigners,' the underlying assumption is that citizens are connected to them, and therefore potential terrorists as well ("Details of Two Surveillance Programs", 2006). This reveals an expanded definition of the terrorist that includes both foreigners *and* citizens.

Overall, 7/7 was seminal in defining terrorist use of the Internet. Today, the Internet is considered instrumental in allowing the terrorist threat to expand beyond the centralized control structure of al-Qaeda networks to one that is self-propagating, decentralized, and inspiring individuals to adopt and disseminate the message of violent extremism – and perhaps be moved to take action by launching an attack at home. This trend has not been limited to the UK and the US The Madrid bombings and subsequent discoveries of terrorist plots planned by citizens in Canada, Denmark, the Netherlands, Spain, and Germany suggest that homegrown terrorism is increasingly part of the topography of terrorism in Western countries – and, according to Sageman (2008), it is largely fuelled by extremists' use of the Internet.

On first consideration, this appears to push Internet governance policy further towards the bordered logic of national security and sovereignty, and suggests a territorialization of the threat that exists within the borders of a given state. With citizens as the source of threat, homegrown terrorism falls within the conventional sphere of domestic law and order, akin to

[92] The NSA was permitted to intercept domestic communications without a warrant in which at least one party – who was a foreign terror suspect or a known terrorist – was located outside of the United States.

the British government's approach to the IRA (c.f. Gregory & Wilkinson, 2005). Confronting that threat is thereby a matter of sovereign jurisdiction.

Yet as political leaders, lawmakers, and intelligence officials persist in saying, the threat is not locally circumscribed. According to a July 2007 US National Intelligence Estimate, homegrown terrorism emerges as a product citizens' capacity to connect – virtually and physically – to "the global extremist movement," which "radicalizes individuals to view the use of violence *here* as legitimate" (qtd. in United States Senate Committee on Homeland Security and Governmental Affairs, 2008, p. 10). Citizens do not radicalize in isolation, but, as the Senate's Report (2008, p. 3) concluded, by "[connecting] with networks throughout the world [that] offer opportunities to build relationships and gain expertise." The threat of terrorism here at home, as former UK Prime Minister Blair (2005) put it, is part of a "global struggle."

In this context, 'global' signifies the planetary reach of terror networks, which is isomorphic with the Internet's diffuse, decentralized architecture, as well as a disruption of the conventional metrics of security: 'global' demonstrates a normative deterritorialization of security by disrupting the assumption that national security is simply about protecting citizens from foreigners. Although it does not remove the importance of protecting borders – the threat from foreigners still remains – it does dislodge the exclusive focus on the 'border' as the line between the space of security (inside the state) and the space of danger (outside the state). This is evident in the US Senate Report (2008, p. 2): "While the United States has appropriately focused its attention at its borders and abroad … Despite these efforts, the violent Islamist threat to the homeland has expanded." With the ability to define threats by distinguishing between citizens and foreigners made problematic, national security has

become tied to a global security logic, whereby the defence of the homeland is about rooting out networks of terror – both at home and abroad. The terminology of homegrown terrorism is in this way ironic: the gaze shifts more and more toward the state because the inside/outside dichotomy of security is no longer tenable – 'homegrown' in fact refers to global terror networks rather than a territorially circumscribed phenomenon. With the Internet playing a central role in this evolution of threat, the global security logic is apparent in the UK 2006 Anti-Terrorism Act and the NSA examples, which have expanded beyond the need to monitor foreign communications to also include the communications of citizens.

Concerns about the pernicious side of global online networks, of course, are not unique to al-Qaeda's move to cyberspace or homegrown terrorism. The commercialization of the Internet has been accompanied by new kinds of 'cybercrime,' such as credit card fraud schemes, spam, etc. Countries have become more attuned to how "criminals are increasingly located in places other than where their acts produce effects" (Council of Europe, 2001b: para. 6).To address this challenge, a number of countries have entered into bilateral and multilateral data-sharing agreements. The most comprehensive of these is the Council of Europe's Convention on Cybercrime.[93] Although the Convention was spurred by concerns about digital copyright infringement, fraud, hacking, and online child pornography, the 9/11 attacks highlighted "the way terrorists use the computers and the Internet to communicate, raise money, recruit and spread propaganda" (Archik, 2003, p. 2). Consequently, the Convention has increasingly been interpreted through the lens of the *global war on terror* (Giacomello, 2004, p. 391). Defining terrorist use of the Internet as a cybercrime

[93] Although the Council's membership is limited to forty-seven European countries (including the Russian Federation, many post-Soviet states, and Turkey), with Japan, the United States, Mexico, Canada, and the Holy See having observer status, the Convention is open for signature to non-member states. APEC and OAS (Organization for American States) leaders have recommended it to its member-states. As of April 2008, 44 countries had signed the Convention, with 22 ratifications.

demonstrates, in a different way, how the *global war on terror* metaphor is providing a normative framework for *global* Internet governance.

The Council of Europe (2001b: para. 6) describes the challenge of addressing crime on the Internet as follows: "the new technologies [in particular the Internet] challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow .... However, domestic laws are generally confined to a specific territory."[94] The Convention accordingly provides tools for locating, gathering, preserving, and sharing computer data across territorial jurisdictions. Specifically, the Convention's ratifying countries agree to harmonized definitions of cybercrime and the domestic measures needed to investigate and prosecute it and accept obligations for extradition and mutual assistance to facilitate cross-border investigations.[95,96]

Although the Convention may appear to be a response to the empirical transcendence of borders, its efficacy ultimately rests in the way it undermines the logic of sovereignty. This is evident in the Convention's Mutual Legal Assistance Treaties [MLATs] (Articles 29-34). These not only require countries to share surveillance data gathered at the national level with law enforcement agencies in different countries, they also authorize a country to request that law enforcement agencies in different jurisdictions monitor on their behalf any of their citizens who are suspected of committing a crime in the requesting country. Outside of requests that flagrantly infringe upon freedom of speech and expression, countries are

[94] Even though the Convention is not limited to the Internet as such, key Council officials claim that the Internet has made the problem of cybercrime more acute (Cangemi, 2004, p. 166).
[95] Articles 2 to 11 (Chapter II) oblige signatory countries to identify illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and digital copyright infringements as criminal offences.
[96] Extradition can be refused on the basis that a) the offence is a political offence, for instance the persecution of freedom of expression, which the requested country deems to be inappropriate, and b) if the requested country claims territorial jurisdiction over the crime. In the latter case, the requested country must submit the case before its authorities. In other words, if it chooses not to extradite, it must prosecute.

obligated to comply, even if the investigated crime is not an offence in both countries (i.e., there is no dual criminality requirement).[97] Although Article 27.4(b) does allow countries to refuse assistance if it "considers that the execution of the request is likely to prejudice its sovereignty, security, *ordre public,* or other essential interests," the Council (2001b: para. 268) argues that the grounds for refusal must be "narrow and exercised with restraint." Effectively, the Convention privileges mutual assistance over sovereignty – in its own words, to the "widest possible extent" (Article 23). The consequence is that surveillance and criminal investigations are detached from their territorial legal frameworks and applied towards the Convention's harmonized definitions and practices. The pressures for global governance therefore arise not only from the planetary reach of Internet communications, but their criminal intent. Put differently, because the Internet removes crime from the domestic sphere – the effects of crime often don't occur where the crimes are performed – the Convention defines the Internet's global space as a criminal zone, necessitating political efforts that contravene the conventional jurisdictional approach to law enforcement.

This disruption of sovereignty through the definition of global space as a criminal domain has opened the Convention to inscription by the *global war on terror* metaphor. Following Article 14(b), which allows the Convention to be applied to any "criminal offences committed by means of a computer system," terrorist use of the Internet can be regarded a cybercrime. The US government, for instance, has in part ratified the Convention because it is seen as an "important [tool] in the battle against terrorism" (Gonzales, 2006). This allows the investigation of terrorist use of the Internet to be party to the Convention's mutual assistance obligations. As US President Bush (2001b) stated shortly after the 9/11 attacks, the elusive nature of terrorist networks means that in order to 'find the terrorists,'

[97] Article 25(5) lists circumstances in which countries may invoke a dual criminality requirement.

countries around the world have "the responsibility to share intelligence and coordinate the efforts of law enforcement." In short, criminalizing terrorist use of the Internet allows governments to investigate the 'loosely affiliated global networks' of terror evolving on the Internet without the conventional territorially based juridical restrictions for investigating crime – hence, the description of the Convention as a tool not just in the fight against cybercrime but also in the battle against terrorism.

In short, terrorist use of the Internet to organize and orchestrate attacks and to radicalize and recruit individuals has made commonplace amongst legislators and intelligence officials the view that "terrorists' centre of gravity lies in the information domain, and it is there that we must engage it" (Dell qtd. in Schmitt & Shanker, 2008). Defining the Internet as a key site for fighting the terrorist threat has inevitably meant that the *global war on terror* metaphor has infused Internet governance with the discourse of national security, underwritten by sovereignty's territorial security premises. Yet the Internet's unique ability to change and modify the nature of the terrorist threat, disrupting the territorially based metric for distinguishing between 'friend' and 'enemy' has made a complete reversion to the principle of sovereignty problematic. As vividly demonstrated in the emerging trend of homegrown terrorism, the threat to national security emanates not only from discretely defined enemies but also a decentralized network of terrorists that includes both citizens and foreigners. The 'global' in the war on terror metaphor accordingly refers both to the planetary reach of terrorist networks – centralized and diffuse – and to a new normative topography of security in which terrorist enemy networks are constituted by familiar 'insiders' as well as foreign 'outsiders.' The description of the Internet within the normative discourse of the *global war on terror* metaphor by lawmakers, political leaders, and

intelligence officials has therefore incorporated the vocabulary of *national security*, *foreigners*, and *border control*. But it must also contend with the vocabulary of *homegrown terrorist*, *global networks of terror*, and the description of the war effort directed *within* and *without*.

The *global war on terror* metaphor reinforces and is juxtaposed against the *state of nature* metaphor and the principle of sovereignty. While protection of the homeland remains the foremost objective, to do so it also attends to a deterritorialized security environment. The incorporated metaphor has therefore defined defending the state as the 'what' of Internet governance; identifying terrorists, and preventing radicalization through surveillance and censorship as the 'how'; Internet communications networks at home and abroad as the 'where'; and law enforcement and intelligence agencies as the 'who.' However, defining the Internet as a 'front' in the *global war on terror* has situated the 'why' of 'national' security within a 'global' security principle. Simply put, the *global war on terror* metaphor invokes the power of sovereignty in order to meet the terrorist threat in its new online domain but terrorists' use of the Internet disrupts the assumptions of sovereignty, demanding, as it were, a *global* security effort for Internet governance.

Defining roles and responsibilities: recruiting ISPs in the fight against global terrorism

As the previous two chapters have demonstrated, the incorporation of a metaphor's political vocabulary opens up a network of action in which different actors are recruited to take on different roles. These roles in turn become consolidated into specific governance institutions. The preceding discussion of the *global war on terror* metaphor's political vocabularies

demonstrates how law enforcement and intelligence officials have had their responsibilities expanded to consider the importance of the Internet in the proliferation of terrorist networks. However, to access the network and monitor its flow of information, Internet surveillance and censorship requires the cooperation of Internet service providers (ISPs), the central nodes for communications flow and data transfer. The inscription of the *global war on terror* metaphor has therefore created a discursive context that sanctions Internet surveillance and censorship as necessary anti-terrorism strategies and such strategies have become consolidated in ISPs' responsibilities for providing information relevant to terrorism investigations.

ISPs emerged as central access points for Internet users as part of the NSF's effort to privatize the NSFNET. In 1994, the NSF pushed forward the 'Project Development Plan' in which the NSF backbone would be replaced by a system of smaller, commercially based operators, each with their own networks. Users would then subscribe, usually for a small fee, to the services provided by these operators and access the Internet by connecting their computers to the operators' networks (Abbate, 1999, pp. 196-200). Because access to the Internet was impossible without subscribing to a smaller operator, the commercially based entities became known as 'Internet service providers' (ISPs). Since then, ISPs have evolved from entities that exclusively provide basic connections to the Internet to include telephone and cable companies, which have bundled multimedia services.

ISPs initially defined themselves according to the 'common carrier' principle and remained neutral towards the content of the communications traffic that passed through their networks. They did however keep records of user activity for 'business purposes.' In the late 1990s, this practice raised privacy concerns – specifically about opportunities for undue

government surveillance or the sale of user preferences to advertising agencies. A series of legislative measures was accordingly implemented that placed strict regulations on the release of user information. User privacy, in other words, was a constraining force on ISP activities (c.f. Kerr, 2003, ft. 143; M. S. Smith, Seifert, McLoughlin, & Moteff, 2002, p. 15).[98]

Despite efforts to maintain their neutrality towards Internet content, growing concerns about cybercrime, especially in advanced industrialized countries, placed ISPs at the centre of debates about the need for greater surveillance and censorship of the Internet. In the US, for instance, copyright concerns produced the 'Online Copyright Limitations and Liability Act' legislated as part of the Digital Millennium Copyright Act (DMCA), which requires ISPs to implement a copyright policy and remove illegal content from its servers when notified about its presence by law enforcement. Pressures for copyright enforcement have recently intensified worldwide and similar efforts are currently underway in the UK, France, and more broadly at the European level,[99] where concerns about child pornography, racism, and hate speech have resulted in partnerships among lawmakers, law enforcement agencies, and ISPs to block and filter 'illegal content' on the Internet (Ramachander, 2008). Although many ISP monitoring activities are conducted voluntarily, perhaps with the exception of the DMCA, studies have shown that ISPs are driven to cooperate with governmental requests in order to prevent legislation that would implement more compulsory surveillance measures

[98] The European Union's Data Protection Directive (1995) and its Directive on Privacy and Electronic Communications (2002) represent two of the most substantive efforts to ensure user privacy.

[99] The UK government has announced that it will introduce legislation requiring ISPs to monitor and take action against any material that infringes on digital copyrights on their servers ("Illegal downloaders 'face UK ban'", 2008). The French government has also unveiled a plan that will mandate all French ISPs to filter material that infringes copyrights ("France unveils anti-piracy plan", 2007). Efforts to create European-wide legislation that would tackle downloading copyrighted material have thus far been defeated. However, digital rights groups have criticized recent amendments to telecommunications legislation, arguing that they make it easier to clamp down on file-sharers (see "MEPs back contested telecoms plan", 2008).

(Ramachander, 2008, p. 186). These changes, argues Geist (2008), reflect a change in the "definition of the appropriate roles and responsibilities of ISPs for the activities that take place on their networks." Because ISPs are the required access points for Internet use, concerns about the nature and content of Internet traffic necessarily implicate the management of their networks, which has challenged their assumed common carrier status. Predictably, this has drawn considerable criticism from privacy advocates.

Since involving ISPs in Internet surveillance and censorship is gaining momentum in other areas of Internet governance, similar efforts in response to terrorist use of the Internet should not be surprising. However, situated in the vocabulary of the *global war on terror* metaphor, they are motivated by different objectives – namely, combating terrorism. While they equally contribute to the sense that any policy to increase state surveillance and censorship territorializes the Internet by placing more and more sectors of Internet governance within the scope of governmental authority (Goldsmith & Wu, 2006), the *global war on terror* metaphor situates this territorialization within a different normative framework – and does not always have a territorializing logic (c.f. Lyon, 2003).

The recruitment of ISPs into the discursive context for Internet governance established by the *global war on terror* metaphor can be delineated in three different areas: data reporting, data retention, and Internet content filtering.

Data Reporting

Data reporting is perhaps the most elementary way to enhance Internet surveillance. It expands the scope of electronic evidence that can be gathered by law enforcement and intelligence agencies, obliging ISPs to provide Internet communications data relevant to the

investigation and detection of terrorism-related activity. Most legislation regarding Internet surveillance – terrorism-related or otherwise – revolves around some kind of data reporting. The PATRIOT Act and the Convention on Cybercrime are two examples of how Internet use within a *global war on terror* requires this activity of ISPs.

a. The PATRIOT ACT

Defined as "an Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement tools and for other purposes," the PATRIOT Act situated the Internet in the discursive context of the fight against terrorism. As stated, the Act updated surveillance law by redefining the classes of information that can be collected in foreign intelligence investigations so that they can, as Ashcroft put, pursue the terrorists in their online environment. The US Communications Storage Act gives law enforcement access to a customer's name, address, phone numbers, billing records, and the list of services used. As noted above, Section 210 of the PATRIOT Act adds to this list session times and durations, assigned network numbers and stored emails. Section 212 also amends previous legislation that prohibited ISPs from knowingly providing subscriber information to government agencies by allowing them to voluntarily turn over subscriber data – including the content of communications – to law enforcement and intelligence agencies in situations where the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." This measure has been largely supported by US ISPs. Recognizing the "importance of electronic evidence … for investigating [terrorism and child abuse]," they feel that in situations of "genuine crisis," previous restrictions have put them in the difficult position of

providing important security information at the cost of violating laws protecting user privacy (US ISPA, 2005).

Reducing ISPs' liability has facilitated their cooperation with law enforcement and security agencies. Sections 225 and Sections 815 of the PATRIOT Act provide greater immunity to ISPs for complying with wiretap orders or governmental requests to preserve data needed in the investigation of a crime or security offence. ISP immunity has more recently come to the fore with the aftermath of the NSA's surveillance program. Charging that telecommunications providers violated consumer privacy by supplying, without a court order, both domestic and international data about customer telephone and email use (which was subsequently used by the NSA to identify terrorist associates), privacy groups, Democratic party members,[100] and other critics of the program argued that ISPs must be held liable for their participation in an illegal government program (Electronic Freedom Foundation, 2008; Risen, 2007). Efforts to allow lawsuits against the participating telecommunications providers were contested on the basis that "foreign intelligence [could] not be conducted without them. But if we continue to subject them to billion dollar lawsuits, we risk losing their cooperation in the future" (Smith qtd. in "US House passes surveillance law", 2008). As a compromise, on 10 July 2008, the US Senate approved a bill passed with bipartisan support in US House of Representatives allowing courts to dismiss any legal action taken against ISPs if the surveillance was requested in writing by the government and that such a request assured them that the surveillance is legal (Lichtblau, 2008a, 2008b). It received presidential approval on the same day.

[100] Democrats did not necessarily contest the idea of asking telecommunications providers to participate in surveillance but wanted to a court to decide whether national security justified their participation. As Senator Patrick Leahy, Chair of the Senate Judiciary Committee, stated, "The issue has never been whether to monitor suspected terrorists but doing it legally and with proper checks and balances to prevent abuses" (qtd. in "US 'to end warrantless wiretaps'", 2007).

One of the more controversial aspects of the PATRIOT Act is its implicit endorsement of 'data sniffing' technologies, such as the FBI's Carnivore system, which are installed directly on ISP servers.[101] Although the FBI abandoned this program in 2005, its termination has fortified ISP cooperation with law enforcement and intelligence agencies. Noting that "available technology" was adequate for FBI needs, the agency announced that it was retiring Carnivore in favour of building more direct partnerships with ISPs who would conduct surveillance on their behalf (Poulsen, 2005).

b. The Convention on Cybercrime

Although the Convention itself is not devised specifically for the Internet, its acute attention to how the Internet exacerbates the effects of cybercrime puts ISPs at the forefront of the Convention's surveillance requirements (see Council of Europe, 2008). The priority placed on ISPs has been further reinforced by the language of *global war on terror*, which defines terrorist use of the Internet as a cybercrime.

The Convention expands ISPs' obligations for Internet surveillance in a number of ways. By harmonizing national laws regarding data collection, ISPs in all signatory countries are required to preserve and disclose Internet traffic data (Article 16)[102] and trace its communication paths (Article 17), and submit stored data, including subscribers to the

[101] Packet-sniffing intercepts specific, pre-identified packets of communications data while they are moving through the ISPs' network, allowing FBI agents to find evidence of criminal activity. A similar scheme was initiated in the United Kingdom with the proposed creation of the National Technical Assistance Centre. This initiative required ISPs to have a "hardwire link directly to [the Centre], thus enabling government 'security operators' to download Internet and email traffic, monitor mobile phone networks and decode encrypted messages" (Demont-Heinrich, 2002, p. 33).

[102] The Convention endorsed preservation over retention in order to strike a balance between concerns about privacy rights and undue burdens placed on ISPs and the need to have the appropriate access to Internet traffic data for the investigation of cybercrime (U.S. ISPA & EuroISPA, 2002). The US government was intimately involved in drafting the Convention. Until 2006 and advocated against data retention policies as a way to combat crime and terrorism on the Internet (Richard, 2005).

services provided by a given ISP (Article 18). Furthermore, Article 19 defines 'computer data' as objects amenable to conventional search and seizure powers and thus Article 20 legalizes the real-time interception of Internet traffic data as it relates to a specific investigation. Further to the harmonization of ISP surveillance requirements across different national jurisdictions, the Convention's MLATs enrol ISPs into its globalized Internet surveillance system. In Articles 29-34, the domestic requirements for preservation, disclosure, search and seizure, and real-time collection of traffic data are applied transnationally for the investigation of crimes committed in one state where communications may have travelled through networks and servers in others. ISPs help local law enforcement agencies conduct Internet surveillance on behalf of authorities located in different countries.

Although the majority of the Convention's requirements focus on providing traffic data such as IP addresses, session times, and subscriber information, in the most serious offences, the Convention permits the collection and interception of content data. As the Council explains, "without the ability to determine and prevent the occurrence of criminality in progress, law enforcement would merely be left with investigating past and completed crimes where the damage has already occurred. Therefore, the real-time interception of content data of computer communications is just as, if not more, important as is the real-time interception of telecommunications" (2001b: para. 228). Surveillance of Internet content is also mandated by the Convention's *Additional Protocol* (2003), which criminalizes the use of the Internet to promote racism and xenophobia. As global terrorism is considered a serious offence, and as many extremist websites contain inflammatory statements regarding different ethnic groups (c.f. I. Black, 2008; Conway, 2007, p. 26), investigations of terrorist use of the Internet conducted under the auspices of the Convention on Cybercrime require ISP

surveillance activities to preserve communications "envelopes" (i.e., IP address origin and destination or URLs) and reveal their content (i.e., text of email messages and content of web pages) both in local settings and for use in investigations elsewhere.

Data Retention

Data retention refers to the routine storage by ISPs of all or large amounts of their communications data. It has been advocated as an important tool in the fight against terrorism since, in the event of an attack, it would allow investigators to go back and search through data that may help to identify terrorists or provide evidence of terror plots that could then be used to prosecute suspects. Data retention differs from data preservation. The latter refers to requests made by law enforcement and intelligence agencies during the course of an investigation to service providers to keep data already in their possession until investigators can procure the appropriate documents that enable the data's disclosure. Data preservation is already a widespread practice in many countries, and is a condition of the Convention on Cybercrime (Article 17). Efforts to promote data retention are more contentious because they require ISPs to expand the scope and duration of the communications data stored. However, these efforts have gained support and momentum in the heightened security context triggered by the 9/11 attacks. In particular, investigators in the UK have noted that access to stored communications data played a part in identifying the suspects in the London bombings. Although already established as a voluntary ISP policy in the UK, following the 7/7 bombings UK officials spearheaded the effort that has resulted in a mandatory data retention directive that applies to all European Union member-states.

Data retention was introduced in the UK in the 2000 Regulatory Investigatory Powers Act to provide law enforcement with the tools to investigate criminal exploitation of the Internet's commercial potential. It was therefore legislated with the "objective of making the UK the best and safest place in the world to conduct and engage in e-commerce" (Straw qtd. in Home Office, 2001). However, in light of findings that the Internet was used to organize the 9/11 attacks, British authorities defended data retention as another way to identify and capture terrorists (Saliban & Sykes, 2002).[103] Consequently, as part of the anti-terrorism efforts legislated in the 2001 Anti-Terrorism, Crime and Security Act, the UK Home Secretary was directed to consult with communications service providers to create a voluntary code of practice for the retention of subscribers' names, email, and IP addresses, sent to and received from email locations, instant messaging handles, log-in names, and time and web activity logs "for the purposes of national security" (Section 102, 3(a)). In the event that this voluntary code was ineffective for law enforcement, the Act gave the Home Secretary the authority to make data retention mandatory.

British ISPs vehemently opposed data retention on the grounds that there was no compelling evidence to suggest that it enhanced national security, that they would be burdened by additional costs, and that by retaining data they were likely to violate privacy laws (Millar, 2003). After failing to forge a consensus with ISPs, the Home Secretary unilaterally issued a voluntary code of practice for data retention in 2003. The *global war on terror* was an explicit motivation: the code of practice was "intended to outline how communications service providers can assist in the fight against terrorism by meeting agreed

[103] Data retention precludes storing the content of communications. Retained URLs, for instance, must be sensitive about revealing content. A visit to http://www.homeoffice.gov.uk/security/terrorism-and-the-law/prevention-of-terrorism/ reveals that the user has accessed material relating to the 2005 Prevention of Terrorism Act. To avoid exposing the content of traffic data, an ISP would store only "http://www/homeoffice.gov.uk"

times for retention of communication data that may be extended beyond those periods for which their individual company currently retains data for business purposes" (Home Office, 2003, "Purpose of the Code").[104] Without the endorsement and support of ISPs, the Home Office claimed it would be forced to implement the mandatory data retention requirements supported by the 2001 anti-terrorism legislation (Millar, 2003). Again, concerns were raised about how a mandatory practice would make ISPs liable for releasing subscriber data and thus vulnerable to being sued by their customers for a breach of privacy laws. Like the PATRIOT Act, if the code had been made mandatory, ISPs would be protected from such liability ("Scrap data retention plans, say MPs", 2003).

Despite threatening to do so, the British government has not instituted mandatory data retention policies within its own legislative frameworks. However, it did spearhead the effort that resulted in a mandatory data retention directive adopted by the European Union in 2006. The US government had already raised concerns about EU data protection policies in the aftermath of the 9/11 attacks. While it did not advocate blanket retention, President Bush did question whether the EU's stringent privacy policies around communications data hindered the identification and capture of terrorists (Foster, 2001). Although this criticism did not trigger any concerted efforts to revise EU data protection policies at the time, it did initiate discussions at the EU level about the potential problems of its data protection and privacy standards in the face of new global terrorist threats. It was only after the 2003 Madrid bombings that the EU acknowledged the "necessity to have rules at EU level that guarantee the availability of traffic data for anti-terrorism purposes" (European Commission, 2005, p.

[104] The Code does address the costs associated with data retention. Although the brunt of the costs are absorbed by service providers, on the basis that the period for retaining data for national security purposes is not significantly larger than the period for retention for business purposes, when for national security reasons there is a request to retain data for a longer period than it would normally be kept for business purposes, the Home Secretary will contribute to a proportion of the marginal costs incurred (Home Office, 2003: para. 23).

2).[105] The London bombings added urgency to this proposal and the EU "reaffirmed … the need to adopt common measures on the retention of telecommunications data as soon as possible" (European Union, 2006: "Preamble"). With considerable pressure from the UK government, the EU Data Retention Directive was adopted on 16 March 2006, with a mandatory retention period of six months to two years. Although the directive was to be implemented within eighteen months of its adoption, its application to the Internet has been extended because of the complexity of the technology required.[106] As a result, UK ISPs will not be affected by the new measures until 2009.

ISPs and privacy advocates have argued against the proposal. Although acknowledging the importance of data retention to address national security threats, ISPs contend that preservation would suffice and that if retention is required, it should be for no longer than six months, in order to reduce the financial burden incurred by retaining data. The EU has argued that the policy is a compromise approach, as law enforcement often needs access to data older than six months in the investigation and prosecution of serious crimes, such as terrorism (European Commission, 2005, p. 5). Privacy advocates contend that the directive's retention period of up to two years is not proportional to the risk and thereby compromises personal privacy and violates Article 8 of the European Human Rights Convention.[107] The Directive, however, notes that Article 8 makes provisions for breaching

[105] There was also a functional need for European-wide data retention. As a number of EU member states were already adopting data retention policies, different legal and technical requirements were creating potential difficulties for the internal market for electronic communications, as ISPs would be faced with different, and even conflicting, requirements for the kind of data retained and under what conditions (European Commission, 2005).

[106] The directive has been criticized for being poorly drafted, without due attention to the technical features of the Internet. One observer has commented that "implementation [of the directive] is practically impossible" (Hosein qtd. in Wakefield, 2007). Others have even claimed that the "legislation has been written by people who didn't understand the internet" (Clayton qtd. in Wakefield, 2007).

[107] Article 8 of the European Convention on Human Rights states that: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public

personal privacy when it relates to national security and law enforcement, thus supporting the objectives behind the data retention policy (European Union, 2006: "Preamble", Section 9).

In light of the EU's directive, data retention has gained support among senior officials in the US Bush Administration, reversing a long-standing preference for data preservation. Although in April 2006 former Attorney General Alberto Gonzales expressed the desire that ISPs retain data solely as a strategy to combat child pornography,[108] shortly after, in a private meeting with major US ISPs in May, Gonzales stated that "we want [data retention] for terrorism" (qtd. in McCullagh, 2006). That the president authorized the NSA to secretly retain data from ISPs to create terrorist profiles is perhaps further evidence that the Bush administration is beginning to favour data retention as an anti-terrorism strategy. To date, US-based ISPs have expressed reservations about data protection, both because of the costs involved and fears of appearing complicit with increased government surveillance on US citizens (*).

Content Filtering

While data reporting and data retention relate to increasing government *surveillance* of the Internet, efforts to combat terrorism have also triggered efforts to expand government *censorship* of the Internet. Content filtering policies are spreading around the world for a

---

authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[108] Claiming that the Internet intensified the problem of child pornography, in a speech to the National Center for Missing and Exploited Children on 20 April 2006, Gonzales stated that the "investigation and prosecution of child predators depends critically on the availability of evidence that is often in the hands of Internet service providers. This evidence will be available for us to use only if the providers retain the records for a reasonable amount of time. Unfortunately, the failure of some Internet service providers to keep records has hampered our ability to conduct investigations in this area." (http://www.usdoj.gov/ag/speeches/2006/ag_speech_060420.html)

variety of reasons. Most prominently, they are associated with "democratically challenged" countries such as China, Iran, and Saudi Arabia, among others, for whom Internet censorship is a way to bolster the government's authority by restricting circulation of materials that might incite political criticism. However, evidence that terrorists use the Internet to communicate with each other and, in particular, to radicalize citizens have accelerated efforts in liberal democratic countries, such as the United States, the United Kingdom, France, Germany, Spain, Italy, Sweden, Denmark, India and many others, to restrict the availability of violent Islamic extremist websites (Deibert, Palfrey, Rohonzinski, & Zittrain, 2008; Drezner, 2004, p. 488). Longstanding concerns about child pornography on the Internet have already led to mandatory content monitoring and blocking by ISPs in many countries, most prominently the UK. Terrorist use of the Internet has, however, expanded the scope of filtering policies and exerted pressures for ISP compliance for security purposes. Especially, although not exclusively, in less democratic countries, the fear of terrorist attacks is used to justify censorship intended for other purposes, such as squashing political dissent (Association for Progressive Communications, 2003).

Inspired by the threat posed by homegrown terrorism, the British government has undertaken some of the most concerted efforts to censor extremist content on the web. From the UK perspective, data retention is a retrospective tool that allows for the investigation of terrorists only *after* an attack. By contrast, the UK government hopes to *prevent* terrorist attacks by "[stopping] people from becoming terrorists or supporting violent extremism" (Cabinet Office, 2008, Section 4.13). Efforts to monitor Internet content were initially instituted in the 2006 Terrorism Act with its specification of new crimes related to the incitement, glorification, and promotion of terrorism. In particular, police are given the

authority to direct ISPs to remove terrorists' statements or articles hosted on their servers. If ISPs fail to take such material down, they can be charged with endorsing or inciting terrorism (JISC Legal, 2007).

The Brown government has bolstered these efforts by attempting to build more collaborative cooperation between ISPs and the government to block extremist content on the Internet. In 2007, the Prime Minister stated that a first priority in the government's attempt to "deal with the challenge posed by terrorism" was to "challenge extremist propaganda." To this end, he announced that the Home Secretary had invited "the largest global technology and internet companies to work together to ensure that our best technical expertise is galvanised to counter incitement to hatred." In January 2008, the Home Secretary announced that she would meet with ISPs to consider "how you can filter out content, how you can work with internet service providers … to get illegal stuff off the Internet" ("Smith targets internet extremism", 2008). Because ISPs have actively cooperated with law enforcement to block child pornography websites, the Home Secretary has announced hopes to garner their support to take similar measures regarding websites that promote terrorism.

UK efforts to censor extremist websites have been supported by efforts at the European level. In light of terrorist plots planned by citizens and residents in Germany, Spain, the Netherlands, and Denmark, the EU has expanded the scope of Internet censorship to include materials that promote terrorism (Frattini, 2007; Ramachander, 2008). A similar strategy is reflected in the Council of Europe's Additional Protocol. To the degree that incitement to terrorism can be considered a form of hate speech, countries that have adopted the Protocol can prosecute terrorist content on the Internet. In 2006, leaders from the six largest European countries met and issued a statement declaring their intention to make the

Internet a "more hostile" place for terrorists by preventing use of the Internet to share information on explosives and to spread propaganda ("Anti-terror plan targets internet ", 2006). In this spirit, initiatives are currently underway to create common policies for targeting extremist content on the Internet at the European level. In a speech introducing the European Union's new counter-terrorism strategy, the European Commissioner responsible for Justice, Freedom and Security, Franco Frattini (2007), stipulated that the Internet was a primary target for anti-terrorism efforts and that policies would be developed that sanctioned the blocking of websites related to bomb-making and incitement to commit terrorists attacks. These efforts will not place new obligations on ISPs for content monitoring, and existing laws that protect ISPs from being liable for monitoring content will remain in place.

With the Internet singled out in the *Violent Radicalization and Homegrown Terrorism Act*, there is growing support among some sectors of the US government for using Internet censorship as an anti-terrorism strategy. However, in the United States censoring extremist content on the Internet has traditionally been met with more resistance. The US Supreme Court, for instance, has ruled that attempts to filter content in the immediate aftermath of 9/11 constituted a violation of US First Amendment rights (Conway, 2007, p. 26). Even the PATRIOT Act, which enhances the government's Internet surveillance powers, explicitly prohibits monitoring of activities that represent an individual's right to free expression.[109] Although the United States has ratified the Convention on Cybercrime, it has opted not to adopt the Convention's Additional Protocol, which limits its options for prosecuting terrorist

[109] See Section 215's amendment to sections of the 1978 Foreign Intelligence Surveillance Act. Following the 9/11 attacks, the FBI amended policies that previously prohibited surveillance of public meetings and spaces. This allowed the FBI to collect "any public" information and "carry out topic research including conducting online searches and accessing online sites and forums" without requiring that the information collected pertain to an ongoing investigation. This access to public information has been criticized for the way in which it possibly infringes on US citizens' First Amendment rights.

content on the Internet. Ironically, because of such protections a significant proportion of terrorist websites are hosted on servers located in the United States (Conway, 2007, p. 26).

Efforts to protect First Amendment rights have not stemmed the effort to censor the Internet. Increasing attention to the use of the Internet to encourage the radicalization of US citizens is galvanizing support for filtering extremist content. Recently, Senator Joseph Lieberman, Chair of the Senate Committee on Homeland Security and Governmental Affairs, which authored the Senate report on the Internet and homegrown terrorism, wrote a letter to Google CEO Eric Schmidt, requesting that it "immediately remove content produced by Islamic terrorist organizations from YouTube" and take action to "prevent them from reappearing" (Lieberman, 2008a). Although eighty or so videos have been removed, the Senator finds this insufficient ("Joe Lieberman, Would be Censor", 2008; Lieberman, 2008b).

Google is not an ISP as such, providing Web services rather than direct access to the Internet. But, making the request to Google does demonstrates the degree to which Internet companies – ISPs or otherwise – are crucial points of control in government attempts to filter Internet content. As Lieberman wrote, "Preventing our citizens from terrorist attacks is a top priority for our government. The private sector can help us do that. By taking action to curtail the use of the YouTube to disseminate [terrorists'] goals and methods, Google will make a singularly important contribution to this important national effort" (Lieberman, 2008a).

Such censorship has been criticized on normative and practical grounds. Privacy and free speech proponents chastise such efforts, seeking to protect the Internet as an open communications medium but also from a fear that vague criteria for filtering content will lead to widespread suppression of content (ACLU, 2008) (c.f. 'Preventing Violent Extremism

Together' Working Groups, 2005, p. 77).[110] Others argue that censorship is a futile exercise. Although government attempts to filter the Internet have become more sophisticated, they are not foolproof and can be easily evaded by hosting extremist websites on private networks or mirror sites (ACLU, 2008; Kohlman, 2006b; OpenNet Initiative, 2007). Still others argue that censorship of the Internet is counterproductive. A report by the Institute of International and European Affairs, for instance, argues that censorship might actually prevent effective identification and pursuit of terrorists and the ability to pre-empt potential attacks. Allowing the content to circulate allows law enforcement and security services to "use websites, chatrooms and forums frequented by Islamist militants and sympathizers for surveillance and intelligence gathering" (Ryan, 2007) (c.f. Kohlman, 2006a, 2006b).

Taken together, the incorporation of the *global war on terror's* political vocabulary has legitimated expanded surveillance and censorship of the Internet as a necessary safeguard against terrorism. Additional policies around data reporting, data retention, and content filtering to combat terrorist use of the Internet have redirected ISP responsibilities towards the investigation and prevention of terrorism, even though such policies contravene ISPs' assumed neutrality toward Internet traffic and content. In the specific context of the *global war on terrorism*, ISPs must now attend to data that might identify terrorists, reveal

[110] Although acknowledging that trend toward radicalization, the 'Preventing Violent Extremism Together' Working Group noted raised concerns about the 2006 Terrorism Act's delineation of acts preparatory to, collecting information pertaining to or glorifying terrorism as criminal offences. The criteria for identifying such acts was criticized for being unclear, with the possibility that "visiting a "jihadist" website could also be in some way criminalised, notwithstanding the fact that visiting a website is obviously completely different to planning 'a serious of act of terrorism'" ('Preventing Violent Extremism Together' Working Groups, 2005, pp. 77-78). The Working Group's report further noted that Association of Chief Police Officers' recommendation for a crime relating to 'inappropriate Internet usage' was "more readily associated with regimes in China and Iran than governments in liberal democracies" (p. 78)

information about terrorists' plots, or circulate content that incites terrorism. ISP cooperation has been procured by guarantees of immunity and protection from liability for compromising user privacy.

ISPs have been recruited into the governance objectives established by the *global war on terror* metaphor because of the Internet's unique role in allowing the terrorist threat to proliferate. While the investigation of terrorism itself is in the hands of law enforcement and security officials, as such investigations increasingly focus on the Internet, they require the active participation of ISPs – indeed, they would be ineffectual without them. Thus, ISPs become black boxes, constituted by law enforcement and security agency directives to investigate terrorism on the Internet. Their public prominence is reflected in the way anti-terrorism directed Internet governance has revolved around defining new surveillance and censorship responsibilities for ISPs. Given the terrorist *use* of the Internet emphasized within the discursive context of the *global war on terror*, ISPs' role as central access points for users also make them the central point of control for Internet monitoring and surveillance – and the public face of the 'who' of Internet governance (c.f. Lessig, 1999). For these reasons, ISPs have become a vital governance institution in the effort to manage the Internet's exploitation by global terrorist networks.

'Secure' performances: the conflicting logics of re- and de- territorialization

According to Geist (2008), the regulatory pressures that have increased ISP responsibilities for surveillance and censorship of the Internet suggest that ISPs are becoming a "private network police." Although he comes to this conclusion by observing that states are

implementing more stringent protections for digital copyright infringements, the recruitment of ISPs in the anti-terrorist effort suggests a similar development, as ISPs are given responsibilities for detecting and reporting terrorist-related Internet communications data and, in some circumstances, blocking content. Shaped and enabled by the *global war on terror* metaphor, these policing activities are designed to meet the metaphor's security objectives. However, this security effort has ushered in greater state involvement in Internet governance by increasing the regulatory pressures on ISPs under the rubric of national security. The metaphor's disruption of the normative assumptions about the enemy has also situated ISP surveillance and censorship within a 'global' security context. Accordingly, the 'security-driven' ISP policing activities ratify both reterritorializing (sovereign) and deterritorializing (global) principles for Internet governance.

Such ratification relies on the repeated *performance* of certain practices by the institutions produced by the incorporation of a metaphor's political vocabulary and their associated networks of action. These practices have a 'governance' function. They not only entail the functional upkeep of the order; in so doing, they also reinforce the metaphor's definition of political reality. Through their routine execution, governance practices continue to inscribe the metaphor as the legitimating principle for political governance and thereby ensure that the political order is reproduced over time. ISPs 'policing' of terrorist use of the Internet signifies the governance practices by which the *global war on terror* and its sovereign and 'global' security impulses remain active as the framework for Internet governance.

As discussed, the PATRIOT Act in the United States, the 2001 Anti-Terrorism, Crime and Security Act and the 2006 Terrorism Act in the United Kingdom, and the use of

the Convention on Cybercrime to define terrorist use of the Internet as a cybercrime have collectively defined the Internet as contributing both to the capacity of terrorists to organize and orchestrate attacks, and the evolution of the threat into a leaderless enterprise with no formal nodes of authority. In this way, they have created the discursive space that specifies ISPs' terrorism-related governance practices. With terrorist use of the Internet accepted as part of the Internet's political reality, and the need to combat it stipulated as a primary objective, collecting and monitoring Internet traffic data and communications has necessitated the cooperation of ISPs. The responsibilities delineated for data reporting, data retention, and content filtering in this way emerge as the governance practices associated with the inscription of the *global war on terror* metaphor in Internet governance. In other words, as terrorist use of the Internet has become accepted as an undisputed 'fact', data reporting, data retention, and filtering of extremist content have been produced as the 'logical' procedures for governing terrorist use of the Internet.

Because these procedures are directed toward combating terrorist use of the Internet, as they are carried out they reinforce the view that the Internet is a place of terrorist activity. ISPs don't make the Internet a more favourable place for terrorists, but their regular surveillance and censorship naturalize the political vocabulary of the *global war on terror* as a way to define a particular dimension of Internet – that is, as a vanguard in the creation and proliferation of global terrorist networks. ISPs are thus continually legitimated as the necessary institutions for securing against terrorist use of the Internet. Accordingly, the prescriptive ethos that surrounds their reporting, retention, and filtering of extremist content is not simply a function of the punitive and coercive authority of the legislative measures that have sanctioned them. By 'performing' the security impulses of the *global war on terror*

metaphor, they normalize the perception of the Internet as a 'terrorist safe haven,' which in turn ensures the regular and repeated deployment of their Internet surveillance and censorship practices.

The performance of these security impulses of the *global war on terror* embodies the tension between the way policy makers, law enforcement and security agents invoke the metaphor to reterritorialize Internet governance, by putting a priority on sovereignty through national security, and the recognition by these same officials that the security threats presented by today's terrorism contravene conventional assumptions about enemies, threats and war and constitute a new global security landscape.

The reterritorializing effort can be detected in several ways. For instance, the initial impetus behind data reporting and retention in the US and UK respectively was to track the way *foreign* terrorists might have used the Internet to plan an attack. Although the Convention on Cybercrime's data reporting requirements could require ISPs in their jurisdictions to provide communications data and to direct law enforcement agencies in other jurisdictions to have their ISPs conduct surveillance on their behalf, this extends the ability of states to collect information pertaining to *national* security. In this way, ISP surveillance in other jurisdictions can be interpreted as an expression of extra-territoriality rather than deterritorialization. Of all the regulatory pressures on ISPs, content filtering seems the most incontrovertible expression of sovereignty. Censorship necessarily infuses a 'bordering' logic on the Internet, with states determining what kind of information comes in and out of their territorial borders. As a response intended to protect citizens from radicalizing influences, this bordering logic is reinforced when ISPs are directed to prioritize national security over the preservation of the Internet as a borderless, open communications platform (i.e. by

contravening the 'common carrier' principle). Indeed, preserving openness is considered a contributing factor in the emergence of the new terrorist threat.

Each of these reterritorializing pressures on ISPs, however, is embedded within the Internet's production of a 'global' security principle, reflected specifically in the rise of homegrown terrorism and the way it complicates the ability to distinguish between 'friends' and 'enemies' on the basis of citizenship. Thus the NSA's request that ISPs collect both foreigner and citizen Internet data to identify any 'domestic' associates of terrorism implicitly suggests that citizens are terrorists and therefore aims at the dispersed and nebulous global terror network. Likewise, the UK's initiative to promote data retention policies at the EU level has been inspired by the realization that the terrorist threat exists 'within' as much as it may infiltrate from 'without.' While the cross-jurisdictional surveillance capacities afforded by the Convention on Cybercrime may buttress the ability of a states to direct ISPs near and far to monitor their networks for the purpose of national security, these surveillance capacities are also enabled by the non-territorially circumscribed definition of criminality. This definition matches the way terrorist use of the Internet contributes to terrorists' capacity to orchestrate attacks and to evolve into a threat without a corporate identity or centralized command structure. ISPs are then uniquely suited for the investigation and potential capture of terrorists located at home and abroad. Ironically, the deterritorializing effects of the *global war on terror* on Internet governance are most prominent in Internet filtering policies. By keeping certain kinds of information 'out,' governments are attempting to thwart the proliferation of global terror networks, where such proliferation refers to the way the Internet can radicalize citizens into terrorist sympathizers.

The bordering logic of content filtering therefore simultaneously enforces the principle of national security and inscribes a deterritorialized definition of threat and enemy.

Effectively, then, reterritorialization and deterritorialization are (contradictory) performative logics of Internet governance shaped by the *global war on terror* metaphor. Associated with protecting national security, the reterritorializing impulse invokes the value of borders by trying to protect citizens from foreign users and radicalizing content. In this way, surveillance and censorship inscribe sovereignty as the legitimating principle of Internet governance. At the same time, the deterritorializing effects of terrorists' use of the Internet to expand terror networks to include both citizens and foreigners has produced a new principle of 'global' security in which foreigners and citizens are both sources of threat. These practices construct the Internet as a global war-zone, in which border control no longer protects against a threat increasingly located at home and abroad. In response, the state has increased its attention to the homeland, not as a result of a sovereign fight against 'foreign' terrorists, but because the state itself has become a site or node within 'global' networks of terror. In sum, the data reporting, data retention, and filtering responsibilities delineated for ISPs by the descriptive frame of the *global war on terror* metaphor are governance practices driven by a securitizing ethos that simultaneously creates pressures for strengthening sovereignty and pushes forward the Internet's global governance.

Overall, terrorism-related data reporting, retention, and filtering have reinforced Internet communications networks as key site of terrorist activity and thus the 'where' of Internet governance. Identifying terrorists and preventing their proliferation through surveillance and censorship have become the means (the 'how') to secure against the terrorist threat. Securing against terrorism ultimately falls into the hands of law enforcement and

security services. However, the sophisticated use of the Internet by terrorists requires the cooperation of ISPs, which have become the 'who' of Internet governance. Although the security objectives inscribed by data reporting, data retention, and filtering constitute the state as the referent object of political governance (the 'what'), the result has not been to inscribe sovereignty as the legitimating principle or the 'why' of Internet governance. Rather, protecting sovereignty has had to attend to how the Internet supports and generates a new 'global' security environment. Consequently, ISPs and surveillance and censorship responsibilities are at once sovereign *and* global institutions and practices of governance

Galvanizing 'security': subverting 'open access,' 'competition,' and 'sovereignty'

Expanding powers of surveillance and censorship as a response to terrorist use of the Internet marks a dramatic shift from the principles of global Internet governance discussed previously. The inscriptive effects of the *global village* and *global marketplace* metaphors are still evident in the IETF and ICANN, for instance, which remain active governance institutions. More broadly, the proliferation of open-source software and peer-to-peer networking demonstrate the degree to which 'open access' remains a valued goal among many Internet users. Online shopping is so commonplace that it would be difficult to understand the average Internet user experience in advanced industrialized countries without it. Despite the way the fight against terrorism has encroached upon the Internet, it does not appear to have delegitimated the normative appeal of *global village* and *global marketplace* metaphors. But that does not mean that they have not been challenged.

Criticism of the *global war on terror* metaphor's effects on Internet governance has been primarily vocalized by privacy and freedom of speech/expression advocates, based on the cyberlibertarian principles associated with the *global village* metaphor. Instead of an indiscriminate opposition to any kind of government regulation of the Internet, they have acknowledged the importance of limited government involvement to combat the proliferation of terrorist networks (M. S. Smith, Seifert, McLoughlin, & Moteff, 2002). The dispute therefore largely rests in the proportion and scope of surveillance and censorship. In the US, for instance, changes to electronic surveillance law introduced by the PATRIOT Act, although geared toward the investigation of 'foreign' threats, have lowered the threshold for surveillance on 'ordinary Americans' (Nijboer 2004).[111] Fears that the government may be encroaching upon the privacy rights of US citizens seem to have been borne out with the exposure of the NSA's domestic surveillance program. US privacy groups have therefore been critical of increased ISP responsibilities for surveillance. Most prominently, they have taken issue with the immunity granted to ISPs and telecommunications providers when asked to provide user information to government agencies (Electronic Freedom Foundation, 2008).

UK privacy groups express a similar concern, arguing that the surveillance measures introduced by recent anti-terrorism legislation suggest that "no longer is Al-Qaeda the main threat, now apparently all UK citizens could be terrorists" (Watson, 2006). Furthermore, critics of the 2006 Terrorism Act have argued that the definition of what constitutes an act to incite or glorify terrorism by use of the Internet is so vague that any number of statements that would normally be protected by freedom of expression laws can now be prosecuted as

[111] The PATRIOT Act changes the Foreign Intelligence Surveillance Act, which allowed surveillance of US citizens only when the 'the' purpose of the investigations was foreign. This rule has been amended so that foreign intelligence could be a 'substantial' but not necessarily the exclusive focus of surveillance on US citizens (Section 218). See also discussion in Jaeger, Bertot and McClure (2003), Kerr (Kerr, 2003),Seamon and Gardner (2005), and Wong (2002).

intent to promote terrorism ('Preventing Violent Extremism Together' Working Groups, 2005, pp. 77-78; Davis qtd. in "New terror law comes into force", 2006). In Europe, privacy advocates have long opposed the data retention directive on the grounds that retention periods imposed on ISPs are too long, and interfere with citizens' rights to privacy. This is considered even more problematic as the finality and aims of data retention have not been clearly specified (European Commission, 2005, p. 5). If privacy advocates have been critical of the way governments have increased their capacities to monitor citizen use of the Internet under the legitimating force of national security, they have been equally, if not more, troubled by the Convention on Cybercrime's MLATs' provisions and lack of dual criminality requirements, which may force governments to enhance Internet surveillance on their own populations, not in their own interests, but on behalf of any other signatory country (EPIC, 2004).

While privacy rights have not been explicitly abandoned by various governments' anti-terrorism-related Internet surveillance and censorship schemes, it appears that a notable shift in priorities has diminished their protection. In fact, despite articulating the need to balance privacy rights with security, privacy protections were added to the PATRIOT Act only when it was renewed in 2005, and even then only as a response to public criticism. Given the measures taken to ensure that ISPs protected user privacy in the mid-to-late 1990s, the more recent deterioration of privacy rights requires explanation. In the European Union, the Data Retention Directive was a significant departure from the 1995 Data Protection Directive, and was justified on the basis that protecting privacy might compromise terrorism investigations.

The normative force of the *global war on terror* metaphor provides distinctive justifications that explain why privacy has fallen to the wayside in terrorism-related Internet governance. Because privacy advocates' criticisms have largely revolved around the way *citizens* have been affected by government efforts to combat terrorist use of the Internet, the *global village* metaphor immediately loses ground to security impulses inscribed by the *global war on terror* metaphor. While the justificatory force of national security puts the emphasis on foreigners, and thus would suggest that citizens should be protected from government efforts to fight terrorism, the rise of homegrown terrorism and the complication of the citizen/foreigner distinction has meant that any citizen could be a terrorist. 'Ordinary' Americans, it turns out, might not be so ordinary and any UK citizen might be a potential terrorist. As a result, it has been necessary to breach privacy laws in order to reveal and uncover which foreigners *and* citizens might be included in 'global' networks of terror – hence, the NSA's *domestic* surveillance program and the UK's attempt to censor the Internet for radical content.

In effect, *global war on terror* has drawn upon the borderless image of the Internet promoted by *global village* advocates, whose conceptions of the Internet as a borderless medium have promoted a more cosmopolitan sense of humanity that transcends the nationalistic conflicts generated by sovereignty. Terrorist use of the Internet has generated a 'borderless' enemy: the sources of threat are domestic as well as foreign. While under the *global village* the Internet is promoted as a space where citizenship and nationality should not matter, terrorist use of the Internet prove this to be the case. Internet terrorism has generated the sense of an 'elusive' enemy, not only in terms of location in space (i.e., a foreigner infiltrating a country) but also in terms of identity (who *is* a possible enemy?). As a

result, blanket surveillance of citizens and foreigners has challenged and, to some degree, subverted the online privacy protections usually accorded citizens. By drawing out the legitimating force of the *global war on terror* metaphor, I am not endorsing the abrogation of privacy, but demonstrating how the misappropriation of the Internet's 'open access' principles has fostered a borderless security environment that generates concerns about national security while also legitimating a new kind of 'global' security framework for Internet governance.

The consequences for the *global marketplace* metaphor have been less clear-cut. Increased government surveillance and the effects on user privacy have been criticized for potentially reducing user confidence in making online purchases, for fear that the government is monitoring their purchases, thereby undermining the commercial potential of the Internet (Tedeschi, 2003). Evidence that online commercial activity has decreased in the wake of government anti-terror measures, however, is as yet inconclusive. A cursory examination would suggest that commercial use of the Internet today has actually increased compared to the period preceding the 9/11 attacks (c.f. M. S. Smith, Seifert, McLoughlin, & Moteff, 2002, pp. 8-9). The displacement of the metaphor is perhaps more evident in the way the tools for investigating commercial crime on the Internet have been redefined and redirected toward the investigation of terrorist use of the Internet, as demonstrated by the application of the Convention on Cybercrime to investigate terrorism. Whether this actually delegitimates the *global marketplace* is contestable. Internet use for financial fraud and other commercial crimes by organized crime circuits and for child pornography had already inflected the metaphor with a 'dark side' (Coyle, 1998; Gray, 1996; Levitsky, 2003; L. Malkin & Elizur, 2001; Whitaker, 2001) To the extent that terrorist use of the Internet is

defined as a criminal activity, especially when terrorist groups have financed their through online credit card scams, online commercial crime and terrorism are listed side by side as reasons for increasing government regulation of the Internet (Richard, 2005). One might even surmise that there is a mutually reinforcing effect between efforts to increase surveillance and censorship as it relates to the commercial aspects of the Internet (for instance, copyright protections) and those directed to combating terrorism.

As stated throughout this chapter, in contrast to the globalizing effect of the *global village* and *global marketplace* discourses, the *global war on terror* metaphor has had more contradictory effects for the normative consequences of sovereignty in Internet governance. Unlike the national security premises and environment of the *state of nature* metaphor, which directed the initial context of Internet development, today's national security environment is a world in which threats are not limited to easily identifiable rival states. The terrorist threat has demonstrated that the enemy can also operate through networks spread across many countries. Initially limited to al-Qaeda, a network with a centralized command structure and corporate identity, terrorist use of the Internet has since confounded conventional metrics of security even further. Its contribution to the growth of homegrown terrorism has globalized the topography of security, so that the notion of 'global' refers to the normative disruption of 'inside' and 'outside' in which citizens and foreigners are both potential enemies. Thus while terrorist use of the Internet has ushered in a return to security, it has not been a complete reversion to sovereignty. The inscription of the *global war on terror* as the legitimating vocabulary of Internet governance has also subverted sovereignty with the introduction of a new principle of 'global' security.

Alternative explanations: **the irony of a *global* war**

In light of arguments that the *global war on terror* metaphor's security impulses herald a return to sovereignty, the principal counter-argument to the position defended in this chapter is that the 'return of the state' in Internet governance signals the end of the Internet's globalization. In this view, the expanded role of the government shows that the Internet is being clawed back and circumscribed within territorial borders and governed according to the principle of sovereignty (c.f. Goldsmith & Wu, 2006). Specifically, this is evidenced through increased pressures on ISPs to carry out government-mandated surveillance and censorship for terrorism related investigations. As an expanding contravention of their common carrier status, it reveals the degree to which sovereign power has encroached upon and co-opted the governance of the Internet. The momentum towards the Internet's global governance has not only slowed, it is potentially being reversed. Despite the 'global' moniker in the *global war on terror* metaphor, the sovereign state is being (re)legitimated as the authoritative locus of Internet governance.

Of course, it would be naïve to dispute that the state has assumed a greater role in terrorism directed Internet governance, as compared to initiatives associated with the *global village* and *global marketplace*. It would also be inaccurate to deny that post-9/11 sovereignty, through the emphasis on 'national' security, has become a discourse tied to Internet governance. Indeed, precisely because foreign terrorists have used the Internet to orchestrate attacks, and because they are increasingly using it to recruit new members, Internet surveillance is one way for states to protect their citizens against a future attack. Hence the changes to the Patriot Act, in which the Internet was tied into the objective of

national security, expressed as the desire to 'unite and strengthen *America*', and the passage of Chapter 11 data retention requirements in the 2001 Anti-Terrorism, Crime and Security Act by UK government as an effort to enhance the safety of *British* businesses and society through "improved protection, tracking and prevention of [international] terrorism."

Yet the delineation of the war in 'global' terms has had consequences that do not necessarily reinforce sovereignty. Specifically, the *global war on terror* metaphor has been consequential in expanding the global governance of the Internet because it has redefined the normative context of war and security. On one level, 'global' signifies the transfiguration of threat and enemy into diffuse networks that cannot be contained in a single state. Because of the Internet's construction as a decentralized system that allows for easy communication across vast distances and the facile publication and dissemination of information by individuals, terrorist use of the Internet for orchestrating attacks and recruiting individuals to the jihadi cause has reinforced the view that when a war is fought against terrorism, the location and identity of the enemy is more difficult to define. ISPs consequently have become crucial in the fight against terrorism: as access points, they provide the practical means by which to monitor the Internet and uncover terrorist networks. This effort takes place nationally, as seen in various legislated surveillance measures, but more importantly transnationally, as evidenced by such things as the Convention on Cybercrime's data collection and sharing requirements.

On another level, because the decentralization of terrorist networks has largely been the result of recruitment of citizens into terror networks – the phenomenon of 'homegrown' terrorism – 'global' also signifies that security is no longer a matter of protecting borders against a 'foreign' threat coming from the 'outside' (even if infiltrating borders): the threat,

as US officials have defined it, "is now increasingly from within" (United States Senate Committee on Homeland Security and Governmental Affairs, 2008, p. 15). As a result, just as important as efforts to eradicate al-Qaeda command centres in Afghanistan, fighting terrorism must happen within the domestic sphere, where terrorist propaganda is compromising the assumed safety of the 'inside' – in the words of British Prime Minister Gordon Brown (2007), the war on terror must be found "at home and abroad." As a result, defined as an anti-terrorism strategy, censorship, at least in Western countries, emerges as a direct response to the shifting categories of war from 'citizens' and 'foreigners' to 'global networks of terror' to 'global civilization'. In short, the normative force of a *global* war on terrorism suggests that sovereign security logics *contend* with globalizing ones – a *global* war complicates sovereignty because the effort to secure the Internet by 'reterritorializing' it under the authority of states ultimately requires that governments adopt categories of war and security that no longer map onto territorial borders.

Reading the involvement of the state in Internet governance as definitive evidence of the return to sovereignty is therefore problematic. An underlying point, reiterated through out this thesis, is that the empirical activity of states is not a metric of sovereignty. Sovereignty is a discourse and thus assessing its influence over the Internet requires determining its legitimating power against metaphors of globalization that deterritorialize political legitimacy. Although the Internet surveillance and censorship practices that the description of the new security context as *global war on terror* have enabled can be read a sovereign response when the enemy can still be defined as a foreigner, as the threat expands and citizens become sources of threat, sovereign legitimacy gives way to a globalizing security ethos: states must identify and thwart global terror networks as they manifest at home and

abroad. Internet governance as shaped by the *global war on terror* has therefore seen a surge in the activity of states. But this has taken place within an evolving global governance framework – where global refers to a new kind of enemy and a new warzone. Barkawi (2006, p. 131) perhaps puts it best, in the global war on terror, "it is still possible to attend to the continuing power and significance of state while also acknowledging the ways in which world politics exceeds territorial states" (Der Derian, 2006; Held & McGrew, 2007; Kaldor, 2006).

Conclusion

In this chapter, I have argued that the *global war on terror* metaphor has created a discursive space in which the Internet has become an important site for tackling the threat of violent Islamic extremism. Noting the ways in which states have responded by bringing the Internet into the realm of *national security*, I have shown the move towards reinscribing sovereignty as the legitimating principle of Internet governance. I have further delineated how terrorist use of the Internet has complicated the conventional metrics of security, which rely on sovereignty's distinction between *citizens* and *foreigners* as well as on *border control*. Citing the growth *homegrown terrorism*, I have examined how the definition of the enemy has expanded beyond both an exclusive focus on rival states and a limited association with al-Qaeda – a shift that has been particularly relevant for Internet governance due to the role of the Internet in the radicalization and recruitment of citizens and the genesis of *global networks of terror*. I have further claimed that the Internet's nexus with contemporary

terrorism also legitimates a new *global security* principle for regulating the Internet so that the terrorist threat can be confronted both *at home and abroad*.

By focusing on the ways in which the metaphor has been adopted and circulated by lawmakers, political leaders, law enforcement, and intelligence agencies in the United States, the United Kingdom, and the Council of Europe, I have shown not only how the Internet has been described as a front in the war on terror but how, as a result, the inscriptive power of the metaphor has influenced governments to increase pressures on ISPs to take on new Internet surveillance and censorship responsibilities. Although Internet surveillance and censorship responsibilities for ISPs are not new, I contend that within the discursive context of the *global war on terror* metaphor, they have a different normative effect. Specifically, I have explored how ISP responsibilities for data reporting, data retention, and filtering of extremist content have become governance practices that have both reterritorialized Internet governance, drawing the Internet toward 'national' security and sovereignty, as well as deterritorialized it, embedding the principle of 'global' security in Internet governance and reinforcing the view that the Internet is a global warzone. In tracing the inscription of the *global war on terror* metaphor, I have considered the conditions that have produced a new set of 'facts' for Internet governance. In particular, I claim that the Internet's communications networks are established as the 'where' of Internet governance, ISPs as the 'who', and identifying and rooting out terrorists through surveillance and censorship as the 'how.' However, based on the metaphor's normative tensions between reterritorialization and deterritorialization, I have argued that the objective of protecting the state – the 'what' – has fostered greater sovereign control of the Internet but also forced the state to amend its activities according to a 'global' security principle. Although security becomes the 'why' of

Internet governance, it is attended by pressures that have continued the Internet's global governance. Overall, I conclude that the *global war on terror* metaphor has inscribed security as the legitimating principle of Internet governance but the conflict between national and 'global' security has pulled Internet governance in different directions, some of which prevent its global governance, but also many of which further it.

Conclusion

Globalization as Global Governance

Few things are permanent in history; and it would be rash
to assume that the territorial unit of power is one of them.
~ E.H. Carr, *The Twenty Years' Crisis*

Stated in brief, the question addressed in this dissertation is *'how and why has the Internet been globalized?'* In answering this question, I have demonstrated that globalization is much more than just the physical diffusion of the Internet's cables, codes and cafés across the planet but the normative constitution of its governance in global terms. Specifically, I have highlighted this feature of globalization by pointing to the circulation of different metaphors of globalization and illuminating how they have influenced the production of global governance by redefining the basis of political legitimacy.

Coming to this conclusion does not dispute the role and significance of the Internet (and through this example, empirical trends associated with globalization more broadly) in our everyday experiences and understandings of globalization; in fact, the Internet is likely what distinguishes contemporary patterns of globalization (Castells, 2000b; Deibert, 1997b; Der Derian, 2003). However, to make the claim that Internet's 'global reach' facilitates the transformation of political order, specifically of the territorially-based sovereign states-system, or more modestly, that it is an exemplar of how globalizing processes have ushered in such transformation, requires more than simply noting the ways in which the Internet easily moves across space in instantaneous time. States are more than just markers of the physical-geographical organization of political authority. They are products of a normative discourse in which a principle of sovereignty legitimates states as the principal and primary

sites of political authority, community and governance. In other words, sovereignty not only describes how political order has been organized into territorial states but why this organization should garner widespread allegiance.

My objective in this dissertation has therefore been to ask globalization scholars to attend to the discursive production of sovereignty. Doing so, however, I find has the consequence of re-framing claims about globalization's transformative impact: if globalization is indeed a moment of profound political change, it requires a set of discourses that challenge the legitimacy sovereignty by legitimating systems of *global* governance. Uncovering these 'discursive dimensions' of globalization has been the motivating impulse and the major contribution of this study. In this concluding chapter, I summarize my theoretical argument and empirical findings and reflect upon their significance for the general study of globalization and global governance and the study of the Internet in International Relations.

Describing and inscribing political metaphors

To locate globalization's discursive dimensions, I have directed my attention to three metaphors of globalization: the *global village*, the *global marketplace* and the *global war on terror*. Although discursive structures are complex, the prevalence of these metaphors provides a lens for exploring globalization's discursive dimensions. Thus, more than demonstrating that these metaphors have pervaded scholarly and popular discussions of globalization and the Internet, I have sought to elaborate upon the roles these metaphors have

played in constituting different patterns of global governance, specifically outlining their contributions to the establishment of new principles of 'global' political legitimacy.

Understanding governance to be how the questions of 'why' governance occurs, 'who' governs, 'where' governance takes place, 'what' is governed and 'how' governance is conducted, are answered, I have explored how metaphors provide the political vocabularies that answer these questions and establish them as the 'facts' of political governance. I have shown that as these 'facts' become embedded and widely disseminated, different actors with disparate interests converge into networks of action that produce 'non-linguistic behaviours', which manifest as the more formal instruments of governance such as laws, institutions, etc. These 'non-linguistic behaviours' are not only the residual effect of the principles of political legitimacy implemented by metaphors' descriptions, just as importantly, they put 'facts' in to action. The answers to the 'why', 'who,' 'what,' 'where' and 'how' of governance not only define a given political order; more significantly, they direct how that order operates. In this way, my discussion of metaphors has made evident that through the activity of its 'non-linguistic behaviours' the metaphor becomes *inscribed* into political thought and action through the development of the everyday 'routines' of governance. This inscription process draws attention to the performative function of metaphors: because governance routines embody a particular system of legitimacy, they become the habitualized activities by which the order is continually constituted. Put simply, governance routines are not only the visible expression of political order – they make visible the principles of legitimacy that constitute that order. Altogether, I have shown that the gradual process of proposing a metaphor, adopting its political vocabulary and creating new governance institutions and routines is how the metaphor becomes 'literalized': from an imaginative and

innovative suggestion, it becomes the definition of political reality and consequently forms the basis of its legitimate governance.

Along these lines, during a moment of political transformation, a literalized metaphor is called into question by a new metaphor, thereby disrupting existing governance routines. This questioning ushers in a 'legitimacy crisis' that makes conditions ripe for the suggestion of a new metaphor. Political change is thus an instance of *metaphorical reinscription*: as a new metaphor comes to describe political order, it puts in place new political vocabularies, triggers new networks of action and institutes new governance routines. In turn, the legitimacy of a previous metaphor is displaced and its political order is replaced as a new metaphor becomes literalized as the normative and empirical framework of governance.

In the context of my study of globalization and the Internet, I have investigated how the *global village*, *global marketplace*, and *global war on terror* metaphors have disrupted the power of the *state of nature* metaphor and its sovereign legitimacy by implementing 'facts' of global Internet governance. Of course, the argument has not been to reduce globalization and global Internet governance to the play and flux of metaphors. However, by highlighting the specific contribution of metaphors within the maelstrom of forces through which political orders are created, dismantled and reconstructed, I have sought to draw out the normative force of globalization discourses in order to show that the consequences of globalization have indeed resulted in political transformation.

***Global village*, *global marketplace*, *global war on terror*: 'open access', 'competition', 'global security' and the legitimation of global Internet governance**

Delimiting the degree to which globalization must exist discursively, I have argued that its 'deterritorializing' effects must relate to more than the movement of information, goods, services and people across territorial borders. Rather, I have claimed that deterritorialization must be a normative discourse that reformulates the legitimating purposes of political order such that it necessitates global governance institutions and practices that reconstitute the spatial organization of politics on a global scale. Accordingly, I have examined how each metaphor of globalization has provide a unique normative discourse of deterritorialization and a new set of facts that globalized the Internet's governance.

In my discussion of the *global village* metaphor, I have demonstrated how sovereignty's normative nexus between *territory*, *authority*, *recognition* and *population* was disrupted and replaced with a new ethos in which *territory* was abandoned as the marker of political community. Humanity became the referent *population*, individual rights and freedoms defined the norms of *recognition*, and the deliberative democratic processes of a global civic society became the mechanisms of political *authority*. As this came to bear upon and become inscribed in the Internet, a new set of governance 'facts' were implemented. In contrast to the practices of 'restricted access' produced by the sovereign security impulses of the *state of nature* metaphor, 'open access' was defended as the legitimating principle and thus the 'why' of global Internet governance, technical standards the 'what', the global Internet user community the 'who', rough-consensus and running code the 'how' and IETF working groups the 'where'. The *global village* metaphor therefore had the effect of deterritorializing the Internet in the literal sense of expanding inter-networked communication beyond the borders of United States but did so with a discourse of

globalization in which open global civic communication was embedded as the primary objective of Internet growth and management.

The popularization of the Internet as a mass communications medium with the introduction of the World Wide Web in conjunction with the privatization of the NSFNET not only disrupted the *global village* metaphor's normative principles of global Internet governance but just as significantly raised further challenges to any remaining sovereign influence in the governance of the Internet. With global market-share displacing *territory* as the metric of political power, *population* was redefined from a set of territorially delimited citizens to a globally dispersed set of consumers. Underwritten by neoliberal approaches to economic growth, *authority* was placed in market mechanisms. *Recognition* accordingly did not rest in the autonomy of governments to delimit specific laws for their national economies. Instead it was afforded to global legal principles that were implemented by governments in their territories to foster and facilitate the expansion of the global market. This contested sovereignty's preference for governing the Internet as 'public resource' and inscribed a new set of 'facts' in which 'competition' became the standard of legitimacy and the 'why' of Internet governance, creating a market for domain names the 'what', a new private corporation, ICANN, as the 'where', its Board of Directors and commercially defined users the 'who' and global trademark law and top-down decision-making the 'how'. Under the inscriptive force of the *global marketplace* metaphor the globalization of the Internet continued apace. But rather than the *global village* metaphor's focus on building a global civic society, this globalization occurred through a normative framework that prized global commerce and consumerism.

Contrary to the interpretation of the 11 September 2001 terrorist attacks as an interruption and potential end of globalization, I have shown that the *global war on terror* is yet another metaphor of globalization. I have argued that its deterritorializing effects can be seen in the redefinition of sovereignty's referents of threat and security. Rather than *territorial* fronts and battlefields, planetary networks become the sites of war. *Populations* are no longer distinguished on the basis of national citizenship but through allegiance to global terrorism or global civilization. *Authority* is indeed visibly expressed in the actions of states and governments but this is not necessarily a result of a return to recognizing their autonomy but instead a view that their conventional security and law enforcement apparatuses can be collectively deployed to combat the new *recognized* enemy-other – global terror networks. The Internet is directly implicated in this definition of globalization. The growing perception that its use for organizational and propaganda purposes has allowed global terror networks to proliferate and conduct attacks has established it as a front in the global fight against terrorism. As a result, the 'facts' of global Internet governance have, although ushering in an effort to enhance national security and protecting the state as the 'what', have also inscribed '*global* security' as the legitimating purpose and the 'why', identifying and rooting out terrorists through Internet surveillance and censorship as the 'how', ISPs as the 'who', and the Internet's globally distributed computer networks the 'where'. Not a simple return to sovereignty and the *state of nature*, the *global war on terror* has embedded the Internet in a global governance framework. But far from the peaceful and profitable principles of the globalization of the Internet under the *global village* and *global marketplace*, the *global war on terror* has globalized the Internet with a more pernicious tenor.

Globalization *as* global governance

From these findings, some broader conclusions can be drawn. Principally, based on a discursive account of political legitimacy, I have argued that globalization must be understood in terms of its empirical processes *and* the normative discourses of deterritorialization that produce global governance principles, institutions, and practices. The transformative effects of globalization on political order can therefore be accounted for by understanding that globalization is a legitimating discourse that shapes and enables the structures of global governance, and evolves as these discourses change.

This discursive approach has several consequences for the study of globalization and global governance within International Relations scholarship. First and foremost, global governance and globalization do not exist as discrete phenomena: globalization must be seen *as* global governance. Global space becomes a site of political authority as a normative vocabulary of deterritorialization establishes the 'facts' that define political reality and unites various actors and initiates specific institutions. The practices of these institutions in turn regulate and reinforce these 'facts,' which ensures that a global political order is reproduced over time. Global governance therefore is not a response to the material challenges of globalization. It is certainly embedded in the empirics of globalization but not because of the geographically dispersed organizational structures of non-state actors. Rather, global governance operates as the productive dynamic through which globalization discourses legitimate 'global' as a normative standpoint for political theory and practice, and subsequently deploys various actors and material factors to construct this space as a site of

politics. The literal transcendence of territorial borders therefore remains important in our definitions of globalization and our analyses of global governance. But to identify how this signals a transformation of *political* order, globalization and global governance must be understood as mutually reinforcing elements of a new principle of political legitimacy.

Understanding globalization *as* global governance has two implications for globalization and global governance theory. First, global governance institutions and practices cannot be dissociated from 'globalization.' Even if they are initially a response to the actual transcendence of territorial borders, global governance institutions and practices are part of the process of transforming political legitimacy beyond sovereignty to produce a new kind of political order. Second, and an outcome of the first, global governance institutions and practices can rightly be said to designate a new political order. However, when they are understood to be shaped and enabled by discourses of globalization, such a claim can be substantiated only by attending to how they produce global space as a site of political authority. Taken together, the observed empirics of globalization – global governance institutions and practices – can be studied as vehicles through which political legitimacy is reconstituted.

The second consequence of a discursive theory of globalization is that the construction of the 'global' political space is open to different deterritorializing discourses. The study of different metaphors of globalization allows for a typology of global governance that accounts for the changing nature of political authority beyond the state and sovereignty, as well as the different ways that global space has been constituted as a site of political authority. This typology suggests another consequence for the study of globalization and global governance. Situating the Internet's global governance within broader debates on

globalization demonstrates that discussions about political order are no longer limited to 'territoriality' (c.f. Steger, 2006). The disruption and displacement of different metaphors of globalization by each other suggests that the principles of global governance do not just contest sovereignty but also advocate different visions and practices of a genuinely *global* politics. A discursive theory of globalization attends to the relative power of global governance institutions against sovereignty as well as the contest between different principles of global political legitimacy.

Globalization studies must also recognize that global governance is not a 'future' possibility. Some scholars contend that the challenge of globalizing processes requires building new kinds of global governance institutions and practices (Archibugi, 2003; Beitz, 2000; Buchanan, 2000; Held, 1995; Linklater, 1998; O. O'Neill, 1986). However, the focus on discourse shows that global governance is already immanent within globalization. Because 'globalization' is embedded in our everyday language and is used as justification for action by policy makers and activists, it is already reconstituting our understandings of political reality. This also has consequences for scholars concerned that emergent global governance institutions contravene principles of justice, fairness and accountability (Archibugi, 2003; Falk, 2008; Falk & Strauss, 2003; Hall & Biersteker, 2002a; Held, 1995; Steffek, 2003; Woods, 1999, 2006). Redressing or reforming global governance institutions requires exposing the *normative* principles that authorize them as sites of power in the first place.

Finally, a discursive theory highlights the role of power in the study of globalization and global governance, which Barnett and Duvall (2005) contend is sorely missing. By examining the production of 'facts,' it draws attention to power's capacity to legitimate a

specific perspective as a principle of political order and establish particular institutions and practices as sites of political authority. The focus on terminal forms of power (or non-linguistic behaviours) connects the micro-processes of political power – discourses and networks of actions – to its macrostructures, where power is exercised through formal sites of political authority. A discursive theory also examines power by examining the asymmetrical effects of a particular vocabulary of deterritorialization. Globalization and global governance are investigated not only for the political positions they legitimate, but also those that are subordinated or excluded. This is a crucial step toward promoting greater collective reflection or dialogue about the need to support or reform global governance institutions and policies.

Overcoming problematic assumptions about the role of the state and the need for universal practices

The position defended in this study is that the Internet, with its planetary reach, is not by definition a matter of global governance. I have shown that from the outset, it was not a 'global' technology, but one developed and defined by the sovereign security impulses of the Cold War and the *state of nature* metaphor. Even after it became a transnational mass communications technology, its governance had varying normative descriptions – *global village*, *global marketplace,* and *global war on terror*. This affects the study of global Internet governance in two ways. The first involves considerations of the state and sovereignty in global Internet governance, and the second pertains to the definition of global governance in the Internet sphere.

The role of the state

My findings question the assumption that because the Internet evolved without government participation, its governance occurs outside of sovereignty's governance logics. My discussion of the *global village* and the IETF, the *global marketplace* and ICANN, and the *global war on terror* and the new security functions of ISPs has shown that states have played an active role in Internet governance – and have even promoted its *global* governance. *The global marketplace* and the creation of a competitive domain name system, for instance, owe much to the efforts of the US Clinton Administration's promotion of electronic commerce. Another example would be how the security-focused roles and responsibilities of ISPs have been defined and constituted by states' reinterpretation of the nature of war, threat, and enemy. These examples show that the state has not disappeared with expansion of the Internet; in some instances, global Internet governance has actually depended on the state.

Furthermore, the Internet has not been naturally immune to sovereign governance. Its global governance has always contended with the legitimating power of sovereignty, and has required disrupting its normative purchase by providing alternative *global* 'facts' of governance. As stated above, the *global village* metaphor deterritorialized the Internet with a discourse that championed open global civic communication rather than 'restricted access'. While the Internet's globalization continued in the context of *global marketplace*, it was through a normative framework that prized borderless commerce and consumerism over 'public resource management.' Although the *global war on terror* has reignited concerns about 'national security' and resulted in attempts to reterritorialize Internet governance, at the

same time, it has disrupted conventional assumptions about the enemy, which has undermined sovereignty and created pressures for a 'global' security effort. The Internet is related to globalization not because it is naturally impervious to sovereignty. On the contrary, its globalization has been achieved through a progressive delegitimation of sovereignty.

Understanding sovereignty as a legitimating discourse rather than a shorthand for state action allows for a better appreciation of the state's role in the Internet's global governance. Indeed, considerations of sovereignty are central to understanding how global governance of the Internet has evolved. However, a discursive theory of globalization shows that even as global Internet governance contests sovereignty, states play an important role. Global Internet governance does not require the absence of states. Rather, analyses must interrogate how states have participated in the "disappearing" legitimacy of sovereignty.

Defining global Internet governance

Demonstrating that the Internet's globalization is in part the product of discursive principles of global governance has consequences for how global Internet governance is defined. The varying effects of different metaphors of globalization demonstrate that neither globalization nor the Internet have a single technical and political structure. Different metaphors produce particular kinds of globalization and global governance; over time, as the prevailing metaphor of globalization changes, so does the Internet's 'global' political potential and governance requirements. The Internet, its globalization, and its global governance are open to capture by different metaphors. Global Internet governance, then, is about the inscription

of globalization discourses into 'ways to speak about' the Internet and their influence on what kind of institutions and practices are deemed necessary to manage the Internet.

Bringing the state 'back in' to discussions of global Internet governance also has consequences for how global Internet governance should be understood. For some, such as Drezner (2004), evidence of active state participation disputes the presumed global governance of the Internet. He argues that states' differing justifications for common practices in Internet regulation – for instance, Internet censorship – fail to produce a coherent basis for global governance. Others argue that national variance is not sufficient to preclude global governance – as long as there is a general similarity between adopted practices on these issues, there is a sufficient basis for global governance – if all countries find it legitimate to censor the Internet, should this not indicate global governance (c.f. Deibert, Palfrey, Rohonzinski, & Zittrain, 2008)? The underlying assumption of these positions is that *global* governance requires universal principles and practices. In their absence, Internet governance is a territorially, state- driven, and 'sovereign' enterprise. Global governance may indeed be manifest in universal principles and practices. But because global governance relies on discourses of globalization that disrupt sovereignty, universality is not a sufficient test of 'global' practices.

Distinguishing 'global' from 'universal' is important for two reasons. First, even if states adopt universal and identical practices for Internet governance, they may do so to enhance their sovereignty over the Internet (Goldsmith & Wu, 2006) – sovereignty, after all, refers to a universally shared set of principles and practices that constitutes an *international* political order. In this case, governance practices may be universal but they undermine the globalization of the Internet. Furthermore, as Drezner notes, states may adopt similar

practices but do so for different political goals. Internet censorship of the Internet in Saudi Arabia, for instance, is directed toward different goals than censorship in the United Kingdom. Thus, similar practices may not demonstrate universal principles. Second, because a discursive theory examines globalization and global governance as a disruption of sovereignty, it shows that differences between national and regional approaches do not dispute the possibility of global governance. It accounts for the uneven distribution of globalization and global governance institutions and practices, and explains that global governance is more concentrated where globalization discourses are more pervasive. For instance, the prevalence and incorporation of the *global war on terror* metaphor in Western liberal democracies can be understood as a basis for global Internet governance in these countries, even though the metaphor has not achieved popularity elsewhere.

Drezner (2004) also argues that where global Internet governance exists, practices and standards reflect state preferences – for example, TCP/IP was adopted in part because states supported it in order to avoid proprietary corporate proposals. Furthermore, even when states defer authority to a non-governmental institution, they retain the power to "intervene to advance their desired ends" (Drezner, 2004, p. 498). To reiterate, global Internet governance does not dispute patterns of state activity but questions whether they can be understood solely as expressions of sovereignty. States may assume active, prominent roles but whether this indicates sovereignty has to be explained rather than assumed. A discursive approach assesses state practices within the legitimating contexts that inform Internet governance – global or sovereignty. The cases discussed in this study have shown that when sovereignty and globalization are studied as discourses, states can be active even when globalization overtakes sovereignty.

Globalization's discursive power suggests that 'global' is not merely a way to describe the Internet's geographical planetary space. Neither does it signify universally adopted practices and institutions of Internet governance. Rather, global Internet governance is about how discourses of globalization disrupt sovereignty and constitute the Internet's global reach as a political space in particular ways.

Implications for International Relations theory: shifting the epistemological and normative focus

The epistemological shift to discourse reframes the study of globalization and global governance International Relations and in turn generates different conclusions about whether and how globalization transforms political order. My objective has been to support globalization proponents claims about globalization's transformative impact but to rectify their overwhelming focus the empirical dimensions of globalization, its transcendence of the physical geography of the state, which treats sovereignty merely as a territorial concept. Because sovereignty is also a *normative* principle that discursively legitimates state authority, simply indicating how empirical processes transcend the physical geography of the state is not enough; analysis must also address how globalizing trends that entail *discursive* reconstitutions of political legitimacy and how these become embedded in new *global* governance institutions and practices. In short, attention to discourse illustrates the normative impact of globalization and provides a more robust way to assess and substantiate its transformative impact. Also, emphasis on the empirical dimensions assumes that the changes underway necessarily relate to a single global system that can be objectively delineated

through new conceptual lenses (Mittleman, 2004; Rosenau, 2003; Ruggie, 1993). My study of metaphors of globalization demonstrates that 'global' itself is subject to variable normative determinations. The transformation of political order beyond sovereignty has not been univocal – a plurality of discourses has evolved over time, each creating different global governance principles, institutions, and practices.

Related to this, the focus on discourse is an attempt to dislodge the conceptual commitment to sovereignty as the 'ordering' principle of world politics. Attention to the discursive constitution of political space through the dominant metaphors of globalization demonstrates how the *normative* purchase of sovereignty is being called into question. My focus on globalization discourses demonstrates that the normative context of state actions and interests is changing; with the rise of global governance institutions and practices, new political agents and structures are emerging. Politics cannot be reduced to sovereignty – continuing state action and prominence in political life does not reflect the normative and conceptual worth of sovereignty. Rather, when globalization is assessed discursively, states are often key proponents and contribute to the transformation of political order beyond sovereignty (Sassen, 2006). Although the power between sovereignty and globalization might be appropriately addressed in relative terms, it is more apt to consider the dynamic between states and globalization relationally.

Contributions of a genealogical method: a conceptual history of globalization

Building from Nietzsche's (1911, p. 180) claim that "truth is but a mobile army of metaphors," I have employed a genealogical method that focuses on the relationship

between power and legitimacy, and examines how existing systems of political power are legitimated through the marginalization of other discourses (Bartelson, 1995; Foucault, 1984; Nietzsche, 1989). This study applies genealogical analysis to uncover the discursive construction of 'global' principles of political legitimacy, their disruption of metaphors of sovereignty and earlier metaphors of globalization, and their consolidation into the more formal sites of political authority. In this way, it accounts for how the legitimating metaphors of sovereign *and* global governance have become embedded and changed over time.

But the genealogical method in this study also furthers a broader objective: the construction of a 'conceptual' history of globalization. Such a history examines the emergence of globalization and global governance as a novel, alternative, and dynamic political discourse – that is, how it provides a different set of metaphors whose impact shifts over time – to sovereignty (and the *state of nature*). Critics may argue that the time frame of this investigation cannot adequately address the issue (Bartelson, 2009; Cosgrove, 2001; Steger, 2008), since it fails to account for the long period in which, despite globalizing processes, the state and sovereignty have remained the referents of political legitimacy and authority (Rosenberg, 2000, pp. 17-43) (Hopkins, 2002). Such criticism, however, considers globalization to be any kind of transboundary processes rather than a specific and unique political vocabulary, which began in the late the late 1950s.[112] It projects the vocabulary of globalization onto a time when it existed either only in a proto-form or did not exist at all. As Bartelson (1995, p. 85) argues, "genealogy must encompass … claims to newness, and take them for what they are: historical events among others. Hence they must be related to and

[112] According to Scholte (2005, pp. 50-51), the first use of 'globalization' to designate a process was in 1959. Two years later, it was included in several dictionaries.

explained with reference to the particular discourse and particular knowledge which engender them."

Others argue that the focus on 'globalization' is dated – that the "age of globalization is over" (Rosenberg, 2005, p. 3). The political enthusiasm, media attention, and acute scholarly interest with which globalization was received during the 1990s may have subsided. However, globalization is not over nor was it simply a fashionable 'buzzword' (c.f. Strange, 1998). Rather, as I have shown, the language of globalization remains pervasive in our everyday discourses; it has become normalized and naturalized in our political vocabulary and embedded in our political practices.

That said, the metaphors explored show that 'globalization' does not have a fixed meaning or definitive structure. A genealogical history also strives to account for how different actors compete and use 'globalization' as a legitimating tool to garner support for their particular political objectives.[113] Such a conceptualization interrogates the origins of 'globalization' as an alternative to sovereignty, as well as how 'globalization' has been redefined, and how this redefinition has altered global governance.

Avenues for future research

This study's discursive theory of globalization and global Internet governance opens up three avenues of future research:

[113] A genealogical approach argues that words do not retain their meaning (Foucault, 1984) (c.f. Bartelson, 1995; Howarth, 1995). Bartelson (1995, p. 13) explains that genealogy builds on the assumption that language, even if deeply entrenched and widely deployed, always operates with ambiguity: "As more and more terms [metaphors and political vocabularies] get linked to central concepts [globalization], the concept becomes saturated with multiple meanings, which imbues it with a certain ambiguity. This ambiguity allows [the concept] to be captured by different interests and deployed to different ends." The multiple metaphors of globalization and global governance exemplify this.

1. *Investigation of globalization's discursive effects and the production of global governance in other areas*. Internet governance is a micro-case of globalization and global governance. However, as globalization theorists suggest, globalization and global governance occur in many areas of political life. This study provides an approach to explore metaphors of globalization in other arenas, such as environmental and financial governance. Comparing micro-cases can reveal how far-reaching the transformative effects of globalization are. The effects need not be identical across cases but they must be isomorphic. Where significant variance exists – i.e., the adoption of globalization discourses in one area and not in another – investigations can delineate the conditions under which a globalization discourse is or is not incorporated. A comparative analysis therefore broadens the study of global political transformation, and deepens its analysis by considering the contexts and conditions influencing the development of global governance institutions and practices.

2. *A multilingual approach*. My analysis has focused on English language metaphors, in part because Internet governance discussions have been conducted primarily in English, and because globalization discourses are more pervasive in Anglo-American countries. However, since vocabularies have normative potentials, it is worth exploring a) the translation of these metaphors into other languages and their effects on globalization, and b) what alternative metaphors exist in other languages and the legitimating principles they promote. The growing demand for a more multilingual Internet makes such an investigation relevant to the study of Internet governance. Of course, the study of multi-lingual metaphors in the globalization discourses is applicable to issues beyond global Internet governance.

3. *Material factors.* This study draws attention to the importance of discursive contexts in the development of global Internet governance, but does not preclude the examination of material factors, such as the Internet's technical architecture. With its focus on enrolment, the theory developed here situates the Internet's technical artefacts within the discursive reconstitution of political order. Similarly, the study of global Internet governance can consider how technologies embody globalization discourses, and how these technologies are used as tools and practices of global governance. Such consideration need not be limited to studies of the Internet: the proliferation of surveillance technologies associated with the *global war on terror* provides another fruitful case study (Amoore, 2007; Lyon, 2003; Monohan, 2006; Sparke, 2006).

Defining globalization as the possibility to conceive of the world as a single global space reflects not only the planetary reach of empirical trends, but also how these trends exist as part of the discursive reconstitution of political space. I have shown that globalization indeed exists as a *deconstructive* process, in which its deterritorializing effects undermine the legitimating power of sovereignty, but that this entails a *reconstructive* process that shapes 'global' political order. Accordingly, I have exposed the power of metaphors of globalization to influence emerging global political order(s). Uncovering their normative vocabularies has theoretical and practical implications. Theoretically, my approach moves beyond a limited focus on how empirical processes cross territorial borders. Rather, it investigates political transformation through a discursive lens, and explores the normative significance of empirical trends. Practically, it provides a way to understand how and why certain policies

and institutional frameworks have become authoritative. Most importantly, this opens up the discursive dimensions of globalization to critical scrutiny, allowing us to identify their impact on global political order, political thought, and action. With this knowledge, we can be more reflective about endorsing, resisting, or transforming the 'global' language we live with and its political effects.

Bibliography

'Preventing Violent Extremism Together' Working Groups. (2005). Working Together to Prevent Violent Extremism (Working Group Report). Retrieved 05 July 2008, from http://www.communities.gov.uk/documents/communities/pdf/152164.pdf

Abbate, J. (1999). *Inventing the Internet*. Cambridge: MIT Press.

Abbate, J. (2001). Government, Business and the Making of the Internet. *Business History Review, 75*(147-176).

Acharya, A. (2007). State Sovereignty After 9/11: Disorganised Hypocrisy. *Political Studies, 55*(2), 274-296.

ACLU. (2008). Coalition Memo to the Senate Committee on Homeland Security and Governmental Affairs Regarding "Homegrown Terrorism". Retrieved 5 July 2008, from http://www.aclu.org/safefree/general/35209leg20080507.html

Agnew, J. (1998). *Geo-politics: Re-visioning World Politics* New York: Routledge.

Agnew, J. (2005). Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics. *Annals of the Association of American Geographers, 95*(2), 437-461.

Agnew, J. (2006a). Globalization has a home address. In D. Conway & N. Heynen (Eds.), *Globalization's Contradictions* (pp. 127-143). Oxon: Routledge.

Agnew, J. (2006b). Globalization has a home address: the geopolitics of globalization. In D. Conway & N. Heynen (Eds.), *Globalization's Contradictions* (pp. 127-143). London: Routledge.

Allen, C. E. (2008). DHS Under Secretary for Intelligence and Analysis Charles E. Allen Address to the Washington Institute for Near East Policy (May 6). from http://www.dhs.gov/xnews/speeches/sp_1210107524856.shtm

Amin, A. (1994). *Post-Fordism: A Reader*. Oxford: Blackwell.

Amoore, L. (2007). Vigilant Visualities. *Security Dialogue, 38*(2), 215-232.

Amoore, L. (Ed.). (2005). *The Global Resistance Reader*. London: Routledge.

Anderson, J. Q. (2005). *Imagining the Internet*. Lanham, MD: Rowman and Littlefield.

Andreas, P. (2003). Redrawing the Line: Borders and Security in the Twenty-first Century. *International Security, 28*(2), 78-111.

Anheiner, H., Galsius, M., & Kaldor, M. (2001). *Global Civil Society Yearbook*. Oxford: Oxford University Press.

Anti-terror plan targets internet [Electronic (2006). Version]. *BBC News*. Retrieved 2 April 2004 from http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/politics/6081850.stm

Archibugi, D. (Ed.). (2003). *Debating Cosmopolitics*. London and New York: Verso.

Archibugi, D., Held, D., & Koehler, M. (Eds.). (1998). *Re-imagining Political Community*. Cambridge: Polity

Archik, K. (2003). Cybercrime: The Council of Europe Convention. In J. V. Blane (Ed.), *Cybercrime and Cyberterrorism: Current Issues* (pp. 2-6). New York: Novinka Books.

Aristotle. (1975). *Art of Rhetoric* (J. H. Freese, Trans.). Cambridge, MA: Harvard University Press.

Aristotle. (1982). *Poetics*. Oxford: Clarendon Press.

Ashcroft, J. (2001). Attorney General John Ashcroft, prepared remarks for the US Mayors Conference. Retrieved 08 October 2008, from http://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10_25.htm

Asprey, W., & Norberg, A. (1988). An Interview with J.C.R. Licklider. *Oral History* Retrieved 7 June 20007

Association for Progressive Communications. (2003). ICT Policy Handbook. Retrieved 12 November 2007, from http://rights.apc.org/handbook/index.shtml

Bajc, V. (2007). Introduction: Debating Surveillance in an Age of Security. *American Behavioral Scientist, 50*(12), 1567-1591.

Barbrook, R. (2008). Re:<nettime> On ARPA's 50th Anniversary [Electronic Version]. *www.nettime.org* - *Nettime mailing list archives*. Retrieved 8 March 2008 from http://www.nettime.org/Lists-Archives/nettime-I-0802/msg00035.html.

Barkawi, T. (2006). *Globalization and War*. Lanham, MD: Rowan and Littlefield.

Barlow, J. P. (1996). Declaration on the Independence of Cyberspace. Retrieved 26 January, 2007, from http://homes.eff.org/~barlow/Declaration-Final.html

Barnes, T. J. (1991). Metaphors and Conversation in Economic Geography: Richard Rorty and the Gravity Model. *Geografiska Annaler, Series B, Human Geography, 73*(2), 111-120.

Barnett, M., & Duvall, R. (2005). Power in global governance. In M. Barnett & R. Duvall (Eds.), *Power in global governance* (pp. 1-32). Cambridge: Cambridge University Press.

Barney, D. (2000). *Prometheus Wired: The Hope for Democracy in an Age of Network Technology*. Chicago: University of Chicago Press.

Barney, D. (2004). *The Network Society*. Cambridge: Polity.

Barsook, P. (1995, October). How Anarchy Works: On location with the masters of metaverse, the Internet Engineering Task Force. *Wired*.

Bartelson, J. (1995). *A Genealogy of Sovereignty*. Cambridge: Cambridge University Press.

Bartelson, J. (2006). Making Sense of Global Civil Society. *European Journal of International Relations, 12*(3), 371-398.

Bartelson, J. (2009). *Visions of World Community*. Cambridge: Cambridge University Press.

Beardsley, M. (1981). The Metaphorical Twist. In M. Johnson (Ed.), *Philosophical Perspectives on Metaphor* (pp. 105-122). Minnesota: University of Minnesota Press.

Beck, U. (1999). *What is Globalization?* Cambridge: Polity.

Beck, U. (2005). *Power in the Global Age*. Cambridge: Polity Press.

Beck, U. (2006). *Cosmopolitan Vision*. Cambridge: Polity.

Beer, F. A., & De Landtsheer, C. l. (Eds.). (2004). *Metaphorical World Politics*. East Lansing, MI: Michigan State University Press.

Beitz, C. (1999). *Political Theory and International Relations* (2nd ed.). Princeton: Princeton University Press.

Beitz, C. (2000). Rawls' Law of Peoples. *Ethics, 110*(4), 669-696.

Bell, D. (1973). *The Coming of the Post-Industrial Society*. New York: Basic Book.

Bellia, P. L. (2003). Surveillance Law Through Cyberlaw's Lens. *The George Washington Law Review, 72*(6), 1375-1458.

Bendrath, R. (2003). The American Cyber-Angst and the Real World - Any Link? In R. Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (pp. 49 - 74). New York: Social Science Research Council.

Bennetto, J., & Herbert, I. (2005). London bombings: the truth emerges [Electronic Version]. *The Independent*. Retrieved 12 April 2008 from

http://www.independent.co.uk/news/uk/crime/london-bombings-the-truth-emerges-502660.html.

Berners-Lee, T. (2000). *Weaving the Web: The Original Design and the Ultimate Destiny of the World Wide Web*. New York: HarperCollins.

Bernstein, S. (2004). The Elusive Basis of Legitimacy in Global Governance: Three Conceptions. *Institute on Globalization and the Human Condition Working Paper Series, GHC 04/02*.

Bernstein, S., & Coleman, W. D. (forthcoming). *Unsettled Legitimacy: Political Community, Power, and Authority in a Global Era*. Vancouver: UBC Press.

Bhagwati, J. (2004). *In Defense of Globalization*. New York: Oxford University Press.

Biersteker, T. J., & Weber, C. (1996a). The social construction of state sovereignty. In T. J. Biersteker & C. Weber (Eds.), *State Sovereignty as Social Construct* (pp. 1-21). Cambridge Cambridge University Press.

Biersteker, T. J., & Weber, C. (Eds.). (1996b). *State Sovereignty as Social Construct*. Cambridge: Cambridge University Press.

Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). Introduction: Common Themes in Sociological and Historical Studies of Technology. In W. E. Bijker, T. P. Hughes & T. Pinch (Eds.), *The Social Construction of Technological Systems* (pp. i-x, 405). Cambridge, MA and London: MIT Press.

Black, I. (2008). Al-Qaida deputy goes online to justify attacks [Electronic Version]. *The Guardian* from www.guardian.co.uk/world/2008/apr/04/alqaida/print.

Black, M. (1979). How Metaphors Work: A Reply to Donald Davidson. In S. Sacks (Ed.), *On Metaphor* (pp. 181-192). Chicago: University of Chicago Press.

Black, M. (1981). Metaphor. In M. Johnson (Ed.), *Philosophical Perspectives on Metaphor* (pp. 63-82). Minnesota: University of Minnesota Press.

Blair, T. (2005). Remarks Delivered at the Labour Party National Conference [16 July]. Retrieved 20 November 2007, from http://news.bbc.co.uk/1/hi/uk/4689363.stm

Blinder, A. S. (1999). Eight Steps for a New Financial Order. *Foreign Affairs, September/October*, 50-63.

Bohman, J., & Lutz-Bachmann, M. (1997). *Perpetual Peace: Essays on Kant's Cosmopolitanism*. Cambridge, MA: MIT Press.

Bono, J. J. (2001). Why Metaphor? Toward a Metaphorics of Scientific Practice. In S. Massen & M. Winterhagen (Eds.), *Science Studies: Probing the Dynamics of Scientific Knowledge* (pp. 213-234). Bielefeld: transcript.

Booth, W. C. (1978). Metaphor of Rhetoric: The Problem of Evaluation. *Critical Inquiry, 5*(1), 49-72.

Bordogna, J. (1997a). Memorandum to Inspector General: Agency Response to OIG Report on the Administration of Internet Addresses. Retrieved 11 October 2007, from http://web.archive.org/web/19990221061833/http://zues.bna.com/e-law/docs/nsfnsi.html

Bordogna, J. (1997b). Testimony Before the House Science Committee Basic Research Subcommittee September 25, 1997. Retrieved 2 April 2008, from http://www.nsf.gov/about/congress/105/jbdomain.jsp

Brachman, J. M. (2006). High-Tech Terror: Al-Qaeda's Use of New Technology. *The Fletcher Forum of World Affairs, 30*(2), 149-164.

Bradner, S. (1996). The Internet Standards Process - Revision 3. *RFC 2026*.

Bradner, S. (1998). IETF Working Group Guidelines and Procedures. *RFC 2418*.

Brassett, J. (2008). Mutiny or Mirror? Politicizing the Limit/Ethics of the Tobin Tax. In M. Kornprobst, V. Pouliot, N. Shah & R. Zaiotti (Eds.), *Metaphors of Globalization: Mirrors, Magicians and Mutinies* (pp. 50-65). Basingstoke: Palgrave.

Brassett, J. (forthcoming). British Irony, Global Justice: A Pragmatic Reading of Chris Brown, Banksy and Ricky Gervais *Review of International Studies*.

Brennan, T. (1997). *At Home in the World: Cosmopolitanism Now*. Cambridge, MA Harvard University Press.

Brenner, N. (2004). *New State Spaces*. New York: Oxford University Press.

Brody, H. (1996). The Web Maestro: An Interview With Tim Berners-Lee. *MIT Technology Review, 99*(5), 32-41.

Brown, G. (2007). Speech to Parliament on Anti-Terrorism Measures [14 November]. Retrieved 18 November 2005, from http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk_politics/7094620.stm

Brown, G. (2008). National Security Strategy statement Retrieved 20 March, 2008, from http://www.number-10.gov.uk/output/Page15102.asp

Buchanan, A. (2000). Rawls' Law of People: rules for a vanished Westphalian order. *Ethics, 110*(4), 697-721.

Bush, G. H. W. (1990). Toward a New World Order [11 September]. Given to a joint session of the United States Congress, Washington, D.C.

Bush, G. W. (2001a). Address to a Joint Session of Congress and the American People [20 September]. Retrieved 08 November 2008, from http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html

Bush, G. W. (2001b). Remarks by the President to the United Nations General Assembly. Retrieved 14 November 2007, from http://www.whitehouse.gov/news/releases/2001/11/print/20011110-3.html

Bush, G. W. (2006). President Bush Discusses NSA Surveillance Program Retrieved 05 August 2008, from http://www.whitehouse.gov/news/releases/2006/05/20060511-1.html

Butler, J. (1990). *Gender Trouble: Feminism and the Subversion of Identity*. New York Routledge.

Cabinet Office. (2008). *The National Security Strategy of the United Kingdom: Security in an interdependent world*. Retrieved. from.

Cairncross, F. (1997). *The Death of Distance: How the Communications Revolution is Changing Our Lives*. London: Orion Publishing Group.

Calder, G. (2003). *Rorty and Redescription*. London: Wiedenfeld and Nicolson.

Callinicos, A. (2005). Imperialism and Global Political Economy. *International Socialism, 2*(108), 109-127.

Cameron, A., & Palan, R. (2004). *The Imagined Economies of Globalization*. London: Sage.

Cangemi, D. (2004). Procedural Law Provisions of the Council of Europe Convention on Cybercrime. *International Review of Law, Computers and Technology, 18*(2), 165-171.

Carr, E. H. (2001). *The Twenty Years' Crisis*. Basingstoke: Palgrave MacMillan.

Castells, M. (2000a). *End of Millennium*. Oxford: Blackwell.

Castells, M. (2000b). *The Rise of the Network Society*. Oxford: Blackwell Publishing.

Castells, M. (2001). *The Internet Galaxy*. Oxford and New York: Oxford University Press.

Castells, M. (2004). *The Power of Identity*. Oxford: Blackwell.

Cerf, V. (1989). Internet Activities Board. *RFC 1120*.

Charteris-Black, J. (2004). *Corpus Approaches to Critical Metaphor Analysis*. Houndsmills: Palgrave MacMillan.

Cheah, P., & Robbins, B. (Eds.). (1998). *Cosmopolitics: Thinking and Feeling Beyond the Nation*. Minneapolis: University of Minnesota Press.

Civil Society Internet Forum. (2000). Civil Society Statement on ICANN Elections. Retrieved 29 October 2007, from http://web.archive.org/web/20010204063800/www.civilsocietyinternetforum.org/statement.html

Clark, C. (2005). Hansard [Electronic Version]. Retrieved 4 April 2008 from www.publications.parliament.uk/pa/cm200506/cmhansrd/vo050720/debtext/50720-04.htm.

Clark, D. D. (1992). "A Cloudy Crystal Ball: Visions of the Future," plenary presentation at 24th meeting of the Internet Engineering Task Force, Cambridge, Mass., 13-17 July. Retrieved 7 July 2006, from http://ietf20.isoc.org/videos/future_ietf_92.pdf

Clark, I. (1999). *Globalization and International Relations Theory*. Oxford: Oxford University Press.

Clausing, J. (1999). Casting Too Wide a Net?; Critics See Internet Board Overstepping Its Authority. *New York Times* Retrieved 18 March 2008, from

http://query.nytimes.com/gst/fullpage.html?res=9D05E1DB1239F934A35755C0A96F958260&sec=&spon=&pagewanted=print

Clifford, M. (2001). *Political Genealogy After Foucault: Savage Identities*. New York and London: Routledge.

Clinton, W. J. (2000). Remarks by the President to the Community of the University of Warwick. Retrieved 25 September 2007, from http://clinton6.nara.gov/2000/12/2000-12-14-remarks-by-the-president-to-the-university-of-warwick.html

Colarik, A. M. (2006). *Cyberterrorism: political and economic implications*. Hershey, PA and London, UK: Idea Group Publishers.

Commission on Global Governance. (1995). *Our Global Neighbourhood*. Oxford: Oxford University Press.

Connolly, W. (1984). Introduction. In W. Connolly (Ed.), *Legitimacy and the State* (pp. 1-18). Oxford: Basil Blackwell.

Conway, M. (2002). What Is Cyberterrorism? *Current History*(December), 436-439.

Conway, M. (2006). Terrorism and the Internet: New Media -- New Threat? *Parliamentary Affairs, 59*(2), 283-298.

Conway, M. (2007). Terrorism and Internet governance: core issues. *Disarmament, 3*(December), 23-33.

Cosgrove, D. (2001). *Apollo's Eye*. Baltimore: John Hopkins University Press.

Council of Europe. (2001a). Convention on Cybercrime. Retrieved 12 August 2006, from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

Council of Europe. (2001b). Convention on Cybercrime - Explanatory Report. Retrieved 23 October 2008, from http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, Concerning the Criminalising of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. Retrieved 23 October 2007, from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

Council of Europe. (2008). Guidelines for the cooperation between law enforcement and internet service providers against cybercrime. Retrieved 4 April 2008, from http://www.coe.int/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp

Cox, R. (1981). Social Forces, States and World Orders: Beyond International Relations Theory. *Millennium: Journal of International Studies, 10*(2), 126-155.

Coyle, D. (1998, 14 May). The dark side of globalization where the black economy thrives. *The Independent,* p. 24.

CPSR. (1993). CPSR Newsletter [Electronic Version], 11. Retrieved 15 August 2007 from www.cpsr.org/prevsite/publications/newsletters/old/1990s/Summer1993.text.

Crocker, D. (1993). Making Standards the IETF Way. *StandardView, 1*(1), 48-53.

Crocker, S. (1969). Documentation Conventions. *RFC 3*.

Crocker, S. (1994). The Process for Organization of Internet Standards Working Group. *RFC 1640*.

Cutler, A. C. (2002). Private international regimes and interfirm cooperation. In R. B. Hall & T. J. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 23-42). Cambridge: Cambridge University Press.

Cutler, A. C., Haufler, V., & Porter, T. (1999). *Private Authority and International Affairs*. Albany, NY: SUNY.

Dalby, S. (1992). Security, Modernity, Ecology: the Dilemmas of Post-Cold War Security Discourse. *Alternatives, 17*(1), 95-134.

Davidson, D. (1978). What Metaphors Mean. *Critical Inquiry, 5*(1), 31-47.

Dean, S. (2003). Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law Under the Patriot Act. *Tulane Journal of Technology and Intellectual Property, 5*, 97-113.

Deibert, R. J. (1997a). 'Exorcismus Theoriae': pragmatism, metaphors and the return of the medieval in IR theory. *European Journal of International Relations, 3*(2), 167-192.

Deibert, R. J. (1997b). *Parchment, Printing and Hypermedia: Communication in World Order Transformation*. New York: Columbia University Press.

Deibert, R. J. (2000). International Plug n' Play: Citizen Activism, the Internet and Global Public Policy. *International Studies Perspectives, 1*(3).

Deibert, R. J. (2003). Black Code: Censorship, Surveillance and the Militarization of Cyberspace. *Millennium: Journal of International Studies, 32*(3), 501-530.

Deibert, R. J., Palfrey, J., Rohonzinski, R., & Zittrain, J. (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, R. J., & Stein, J. (2003). Social and Electronic Networks in the War on Terror. In R. Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York, New York: Social Science Research Council.

Demont-Heinrich, C. (2002). Central points of control and surveillance on a 'decentralized' Net. *Info, 4*(4), 32-42.

Denning, D. E. (2000). Cyberterrorism. Testimony before the Special Oversight Committee on Terrorism, Committee on Armed Services, U.S. House of Representatives (23 May). Retrieved 18 November 2007, from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Denning, D. E. (2001). Is Cyber Terror Next? *Social Science Research Council / After Sept. 11* Retrieved 15 November 2007, from http://www.ssrc.org/sept11/essays/denning_text_only.htm

Der Derian, J. (2003). The Question of Information Technology in International Relations. *Millennium: Journal of International Studies, 32*(3), 441-456.

Der Derian, J. (2006). How should sovereignty be defended? . In C. Bickerton, P. Cunliffe & A. Gourevitch (Eds.), *Politics Without Sovereignty* (pp. 187-204). London: UCL Press.

Details of Two Surveillance Programs [Electronic (2006). Version]. *New York Times*, 14 May. Retrieved 16 April 2008 from http://www.nytimes.com/2006/05/14/washington/14nsabox.html?scp=1&sq=Details%20of%20Two%20Surveillance%20Programs&st=cse.

Devetak, R. (2001). Postmodernism. In S. Burchill (Ed.), *Theories of International Relations* (pp. 181-208). Basingstoke and New York: Palgrave.

Dodge, M., & Kitchin, R. (1998). *Mapping Cyberspace*. London: Routledge.

Drake, W. J. (1993). The Internet religious war. *Telecommunications Policy* 643-649.

Drake, W. J. (2004). Reframing Internet Governance Discourse: Fifteen Baseline Propositions. In D. MacLean (Ed.), *Internet Governance: A Grand Collaboration* (pp. 122-161). New York: United Nations ICT Task Force.

Drezner, D. (2004). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly, 119*(3), 477-498.

Dueker, K. S. (1996). Trademark Law Lost in Cyberspace: Trademark Protection for Internet Addresses. *Harvard Journal of Law and Technology, 9*(2), 483-512.

Dunne, T., & Wheeler, N. (2001). East Timor and the new humanitarian interventionism . *International Affairs, 77*(4), 805-827.

Edge, D. (1974). Technological Metaphor and Social Control. *New Literary History, 6*((Special Issue)), 135-147.

Eichengreen, B. (1999). *Toward a New International Financial Architecture: A Practical Post-Asia Agenda*. Washington: Institute for International Economics.

Electronic Freedom Foundation. (2008). The Case Against Retroactive Immunity for Telecoms. from http://www.eff.org/nsa

Elmer-DeWitt, P. (1993). Take A Trip into the Future on the ELECTRONIC SUPERHIGHWAY [Electronic Version]. *Time* from http://www.time.com/time/magazine/article/0,9171,978216-3,00.html.

Elmer-DeWitt, P. (1995). Welcome to Cyberspace. *Time, Spring,* 4-11.

EPIC. (2004). Letter: Senate Committee on Foreign Relations Regarding Convention on Cybercrime (June 14). Retrieved 10 October 2007, from http://epic.org/privacy/intl/senateletter-061704.pdf

Eschle, C., & Maiguashca, B. (Eds.). (2005). *Critical Theories, International Relations and 'the Anti-Globalisation Movement'*. London: Routledge.

Ess, C. (1998). Cosmopolitan Ideal or Cybercentrism: A Critical Examination of the Underlying Assumptions of "The Electronic Global Village" [Electronic Version]. *APA Newsletters*, 97. Retrieved 10 March 2008 from http://www.apaonline.org/apa/archive/newsletters/v97n2/computers/ess.asp.

European Commission. (2005). Explanatory Memorandum - Proposal for a Directive of the European Parliament and of the Council on the retention of data processes in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:EN:PDF

European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals on the processing of personal data and on the free movement of such data *Official Journal of the European Communities, No L 281*(23 November), 31-50.

European Union. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Communities, L 201*(31 July), 37-47.

European Union. (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications

services or of public communications networks and amending Directive 2002/58/EC. *Official Journal of the European Communities, L 105*(13 April), 54-63.

Executive Summary of E-Commerce Report [Electronic (1997). Version]. *Global Issues*, 2 (4). Retrieved 10 October 2008 from http://usinfo.state.gov/journals/itgic/1097/ijge/gj-12.htm.

Fairclough, N. (2001). Critical Discourse Analysis as a method in social scientific research. In R. Wodak & M. Meyer (Eds.), *Methods of Critical Discourse Analysis* (pp. 121-138). London: Sage.

Fairclough, N. (2006). *Globalization and Language*. London: Routledge.

Falk, R. (2008). Where is 'The Fork in the Road'? Over the Horizon! An Inquiry into the Failure of UN Reform. In M. Kornprobst, V. Pouliot, N. Shah & R. Zaiotti (Eds.), *Metaphors of Globalization: Mirrors, Magicians and Mutinies*. Basingstoke: Palgrave.

Falk, R., & Strauss, A. (2003). The Deeper Challenges of Global Terrorism: A Democratizing Response. In D. Archibugi (Ed.), *Cosmopolitics* (pp. 203-231). London and New York: Verso.

Ferguson, M. (1992). The Mythology of Globalization. *European Journal of Communications, 7*(1), 69-93.

Ferguson, N. (2004). *Colossus*. New York: Penguin Books.

Ferguson, Y. H., & Mansbach, R. W. (2004). *Remapping Global Politics*. Cambridge: Cambridge University Press.

Fisher, W. F., & Ponniah, T. (Eds.). (2003). *Another World is Possible*. London and New York: Zed Books.

Flichy, P. (2007). *The Internet Imaginaire*. Cambridge, Massachusetts: MIT Press.

Foreign Policy. (2007). Globalization Index [Electronic Version]. *Foreign Policy*. Retrieved 12 September from http://www.foreignpolicy.com/story/cms.php?story_id=3995.

Foster, J. (2001). Letter: United States Mission to the European Union. Retrieved 05 August 2008, from http://www.statewatch.org/news/2001/nov/06Ausalet.htm

Foucault, M. (1972). *Archaeology of Knowledge*. London: Tavistock Publications.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison* (A. Sheridan, Trans.). New York: Vintage

Foucault, M. (1978). *The History of Sexuality: An Introduction* (R. Hurley, Trans. Vol. 1). New York: Vintage.

Foucault, M. (1984). Nietzsche, Genealogy, History. In P. Rabinow (Ed.), *The Foucault Reader* (pp. 76-100). New York: Pantheon Books.

Foucault, M. (2000). Governmentality. In J. D. Faubion (Ed.), *Michel Foucault: Power* (pp. 201-222). New York: The New Press.

Framework for Global Electronic Commerce. (1996). Retrieved. from http://www.technology.gov/digeconomy/11.htm.

Framework for Global Electronic Commerce. (1997). Retrieved. from http://www.technology.gov/digeconomy/11.htm.

France unveils anti-piracy plan [Electronic (2007). Version]. *BBC News*, 23 November. Retrieved 11 April 2008 from http://news.bbc.co.uk/2/hi/technology/7110024.stm

Frattini, F. (2007). EU Counter-terrorism strategy (Speech Delivered to the European Parliament 5 September). Retrieved 11 November 2007, from

http://europe.eu/rapid/pressReleaseAction.do?reference=SPEECH/07/05/505&format=HTML&aged=l&language=EN&guiLanguage=en

Friedman, T. L. (2000). *The Lexus and the Olive Tree*. New York: Anchor Publications.

Friedman, T. L. (2005). *The World Is Flat*. New York: Farrar, Strauss and Giroux.

Frissen, P. (1997). The virtual state: postmodernisation, informationisation and public administration. In B. D. Loader (Ed.), *The Governance of Cyberspace: Politics, technology and global restructuring* (pp. 111-125). London: Routledge.

Froomkin, M. (2003). Habermas@discourse.net: toward a critical theory of cyberspace. *Harvard Law Review, 116*(3), 751-873.

Fukuyama, F. (1992). *The end of history and the last man*: Free Press.

Fuller, B. (1970). *Operating Manual for Spaceship Earth*. New York: Simon and Schuster.

Galloway, A. R. (2004). *Protocol*. Cambridge: MIT Press.

Galvin, J. (1996). IAB and IESG Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees. *RFC 2027*.

Geist, M. (2008). ISPs new role in network control [Electronic Version]. *BBC News*, 29 January. Retrieved 17 July 2008 from http://news.bbc.co.uk/2/hi/technology/7215235.stm.

Giacomello, G. (2004). Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism. *Studies in Conflict and Terrorism, 27*(5), 387-408.

Gill, S. (1995). Globalisation, Market Civilisation and Disciplinary Neoliberalism. *Millennium: Journal of International Studies, 24*(3), 399-423.

Goatley, A. (1997). *The Language of Metaphors*. London: Routledge.

Godwin, M. (2003). *Cyber Rights: Defending Free Speech in the Digital Age*. Cambridge, MA: MIT Press.

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

Gonzales, A. R. (2006). Statement of Attorney General Alberto R. Gonzales on the Passage of the Cybercrime Convention. Retrieved 13 November 2007, from http://www.usdoj.gov/opa/pr/2006/August/06_ag_499.hyml

Goodman, N. (1981). Languages of Art. In M. Johnson (Ed.), *Philosophical Perspectives on Metaphor* (pp. 123-135). Minneapolis: University of Minnesota Press.

Government of the United Kingdom. (2001). The Anti-Crime, Terrorism and Security Act. Retrieved 10 October 2008, from http://www.opsi.gov.uk/acts/acts2001/ukpga_20010024_en_1

Government of the United Kingdom. (2006). Terrorism Act 2006. Retrieved 10 October 2008, from http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_1

Gray, J. (1996). Globalization - the dark side. *New Statesman, 127*(4376), 32.

Gray, J. (2002). The End of Globalization [Electronic Version]. *Resurgence*, 212. Retrieved 8 August 2007 from http://www.resurgence.org/resurgence/issues/gray212.htm.

Gregory, F., & Wilkinson, P. (2005). Security, Terrorism and the UK *Chatham House Briefing Paper, ISP/NSCBriefing Paper 05/01* 1-8.

Habermas, J. (1973). *Legitimation Crisis* (T. McCarthy, Trans.). Boston: Beacon Press.

Hafner, A., & Lyon, M. (1996). *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon and Schuster.

Hafner, A., & Lyon, M. (1998). *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon and Schuster.

Hale, D. G. (1971). *The Body Politic: A Political Metaphor in Renaissance English Literature*. The Hague and Paris: Mouton.

Hall, R. B., & Biersteker, T. J. (2002a). The emergence of private authority in the international system. In R. B. Hall & T. J. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 3 - 22). Cambridge: Cambridge University Press.

Hall, R. B., & Biersteker, T. J. (Eds.). (2002b). *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press.

Hansen, L. (2006). *Security as Practice: Discourse Analysis and the Bosnian War*. Oxford and New York Routledge.

Hardt, M., & Negri, A. (2000). *Empire*. Cambridge, MA: Harvard University Press.

Hardt, M., & Negri, A. (2004). *Multitude: war and Democracy in the Age of Empire*. New York: Penguin Books.

Harmes, A. (2006). Neoliberalism and multilevel governance *Review of International Political Economy, 13*(5), 725-749.

Harmon, A. (1998). U.S. Expected to Support Shift in Administration of the Internet. *New York Times* Retrieved 18 March 2008, from http://http://query.nytimes.com/gst/fullpage.html?res=9D05E1DC143DF933A15753C1A96E958260&sec=&spon=&pagewanted=print

Harvey, D. (2005a). *A Brief History of Neoliberalism*. New York: Oxford University Press.

Harvey, D. (2005b). From Globalization to the New Imperialism. In R. P. Appelbaum & W. I. Robinson (Eds.), *Critical Globalization Studies* (pp. 91-100). New York and London: Routledge.

Hauben, M., & Hauben, R. (1997). *Netizens: On the History and Impact of the Usenet and the Internet*. Los Alamitos, CA: IEEE Computer Society Press.

Hauben, R. (2008). ARPA's 50th Anniversary and the Internet: a Model for Basic Change [Electronic Version]. *tazblog: Netizen Journalism and the New News*. Retrieved 4 March 2008 from http://taz.de/blogs/netizenblog/2008/02/12/arpas-50th-anniversary-and-the-internet-a-model-for-basic-research/.

Hawkes, T. (1972). *Metaphor*. London: Metheren and Co. Ltd.

Held, D. (1995). *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance*. Stanford: Stanford University Press.

Held, D. (2004). *The Global Covenant*. Cambridge: Polity.

Held, D., & McGrew, A. (2002). *Globalization/Anti-Globalization*. Cambridge: Polity Press.

Held, D., & McGrew, A. (2007). Globalization at Risk? . In D. Held & A. McGrew (Eds.), *Globalization Theory: Approaches and Controversies* (pp. 1-14). Cambridge: Polity Press.

Held, D., McGrew, A., Goldblatt, D., & Perraton, J. (1999). *Global Transformations: Politics, Economics and Culture*. Cambridge: Polity Press.

Herzfeld, C. (2008). How the change agent has changed. *Nature, 451*, 403-404.

Hesse, M. (1980). *Revolutions and Reconstructions in the Philosophy of Science*. Bloomington: Indiana University Press.

Hesse, M. (1987). Tropical Talk: The Myth of the Literal. *Proceedings of the Aristotelian Society, Supplementary Volume*(LXI), 297-311.

Hirst, P., & Thompson, G. (1999). *Globalization in Question*. Cambridge: Polity Press.

Hobbes, T. (1996). *Leviathan*. Cambridge: Cambridge University Press.

Hobson, J. (2007). Sovereignty Post-9/11. *Political Studies, 55*(2), 271-273.

Hofmann, J. (2005). Internet Governance: A Regulative Idea in Flux (pp. 1-25): Social Science Research Centre Berlin.

Home Office. (2001). Head of National Technical Assistance Centre (NTAC) Announce [Electronic Version]. *Home Office News Release*, 30/03/2001. Retrieved 6 April 2008 from http://www.cyber-rights.org/documents/ntac.htm

Home Office. (2003). Retention of Communications Data Under Part 11: Anti-Terrorism, Crime and Security Act 2001 - Voluntary Code of Practice. Retrieved 4 April 2008, from http://security.homeoffice.gov.uk/news-publications/publication-search/general/5b1.pdf

Hopkins, A. G. (Ed.). (2002). *Globalization in World History*. New York: W.W. Norton.

Hovey, R., & Bradner, S. (1996). Organizations Involved in the IETF Standards Process. *RFC 2028*.

Howarth, D. (1995). Discourse Theory. In D. Marsh & G. Stoker (Eds.), *Theory and Method in Political Science* (pp. 115-133). Basingstoke: MacMillan.

IETF Secretariat, CNRI, & Malkin, G. (1994). The Tao of IETF: A Guide for New Attendees of the Internet Engineering Task Force. *RFC 1718*.

Illegal downloaders 'face UK ban' [Electronic (2008). Version]. *BBC News*, 12 February. Retrieved 12 February 20008 from http://news.bbc.co.uk/2/hi/business/7240234.stm

International Ad Hoc Committee. (1997). Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs. Retrieved 20 February 2007, from http://www.gtld-mou.org/draft-iahc-recommend-00.html

Internet Activities Board. (1992). The Internet Standards Process. *RFC 1310*.

Internet Architecture Board, & Internet Engineering Steering Group. (1994). The Internet Standards Process - Revision 2. *RFC 1602*.

Internet Corporation for Assigned Names and Numbers. (1998a). Articles of Incorporation of Internet Corporation For Assigned Names and Numbers. Retrieved 23 March 2008, from www.icann.org/general/articles.htm

Internet Corporation for Assigned Names and Numbers. (1998b). Bylaws for Internet Corporation for Assigned Names and Numbers (As effective 6 November 1998). Retrieved 23 March 2008, from http://www.icann.org/general/archive-bylaws/bylaws-06nov98

Internet Corporation for Assigned Names and Numbers. (1998c). Bylaws for Internet Corporation for Assigned Names and Numbers (As effective 21 November 1998). Retrieved 23 March 2008, from http://www.icann.org/general/archive-bylaws/bylaws-23nov98.htm

Internet Corporation for Assigned Names and Numbers. (1999a). Bylaws for Internet Corporation for Assigned Names and Numbers (As Amended and Revised 29 October 1999). Retrieved 23 March 2008, from http://www.icann.org/general/archive-bylaws/bylaws-16jul00.htm

Internet Corporation for Assigned Names and Numbers. (1999b). Bylaws for Internet Corporation for Assigned Names and Numbers (As Revised March 31, 1999). Retrieved 23 March 2008, from http://www.icann.org/general/archive-bylaws/bylaws-31mar99.htm

Internet Corporation for Assigned Names and Numbers. (2000). Uniform Domain-Name Dispute-Resolution Policy. Retrieved 23 March 2008, from http://www.icann.org/udrp/udrp.htm

Internet Society. (1992). ISOC Mission and Strategic Plan. Retrieved 2 October 2006, from http://www.isoc.org/isoc/mission/

Internet Society. (1995). A "Proposal for an ISOC Role in the DNS Name Space Management". Retrieved 26 October 2007, from http://www.web.archive.org/19970227101521/http://iiia.org/newdom/1995q4/0154.html

Jackson, R. (2005). *Writing the War on Terrorism*. Manchester: Manchester University Press.

Jackson, R. (2007). Sovereignty and its Presuppositions: Before 9/11 and After. *Political Studies, 55*(2), 297-317.

Jaeger, P. T., Bertot, J. C., & McClure, C. R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly, 20*, 295-314.

JISC Legal. (2007). ISA Liability - Overview. Retrieved 4 April 2008, from http://www.jisclegal.ac.uk/ispliability/ispliability.htm

Joe Lieberman, Would be Censor [Electronic (2008). Version]. *New York Times*, 25 May from

http://www.nytimes.com/2008/05/25/opinion/25sun1.html?scp=1&sq=Lieberman%20YouTube&st=cse.

Johnson, M. (Ed.). (1981). *Philosophical Perspectives on Metaphor*. Minnesota: University of Minnesota Press.

Jones, K. C. (2005). Feds Say Computer Surveillance Hindered Without Patriot Act [Electronic Version]. *techweb network* from http://www.techweb.com/article/printableArticle.jhtml?articleID-175007552&site_section=700028.

Kaldor, M. (2006). *New and Old Wars* (2nd ed.). Cambridge: Polity Press.

Kant, I. (1996). Towards a Perpetual Peace. In M. Gordon (Ed.), *The Cambridge Edition of the Works of Immanuel Kant* (pp. 311-352). Cambridge: Cambridge University Press.

Kantorowicz, E. H. (1957). *The King's Two Bodies: A Study in Medieval Political Theology*. Princeton, NJ: Princeton University Press.

Katz, J. (1997). The Digital Citizen [Electronic Version]. *Wired*, 5. Retrieved 5 March 2008 from http://www.wired.com/wired/archive/5.12/netizen_pr.html.

Katz, R., & Devon, J. (2007). Web of Terror [Electronic Version]. *Forbes.com* from http://members.forbes.com/forbes/2007/0507/1849.com.

Keck, M. E., & Sikkink, K. (1998). *Activists Beyond Borders: Advocacy Networks in International Politics*. Ithaca: Cornell University Press.

Keohane, R. O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Kerr, O. S. (2003). Internet surveillance law of the USA Patriot Act: The big brother that isn't. *Northwestern University Law Review, 97*(2), 607-673.

King, D. C. (1970). Freedom in the Global Village [Electronic Version]. *The Freeman: Ideas on Liberty*, 20. Retrieved 8 March 2008 from http://www.fee.org/Publications/the-Freeman/article.asp?aid=6668.

Kirby, A. (2007). The London Bombers as "Self-Starters": A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques. *Studies in Conflict and Terrorism, 30*(5), 415-428.

Kissinger, H. (2008). Globalization and its Discontents [Electronic Version]. *International Herald Tribune*. Retrieved 6 June 200.

Kittay, E. F. (1987). *Metaphor: Its Cognitive Force and Linguistic Structure*. Oxford: Clarendon Press.

Klein, H. (2001). The feasibility of global democracy: understanding ICANN's at-large election. *Info, 3*(4), 333-345.

Klein, N. (2002). *Fences and Windows*. Toronto: Vintage Canada.

Kobrin, S. J. (1998). The MAI and the Clash of Globalization. *Foreign Policy*(Fall), 97-109.

Kobrin, S. J. (2002). Economic governance in an electronically networked global economy. In R. B. Hall & T. J. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 43-75). Cambridge: Cambridge University Press.

Kohlman, E. (2006a). The Real Online Threat. *Foreign Affairs, 85*(5), 115.

Kohlman, E. (2006b). Weighing the Terrorist Threat on the Internet, *Interview with National Public Radio (26 August)*.

Kornprobst, M., Pouliot, V., Shah, N., & Zaiotti, R. (Eds.). (2008). *Metaphors of Globalization: Mirrors, Magicians and Mutinies*. Basingstoke: Palgrave.

Krasner, S. (1999). *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press.

Kratochwil, F. (1991). *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*. Cambridge: Cambridge University Press.

Kratochwil, F. (1995). Sovereignty as Dominion: Is There a Right of Humanitarian Intervention

. In G. Lyons & M. Mastandano (Eds.), *Beyond Westphalia?* (pp. 21-42). Baltimore: Johns Hopkins University Press.

Krishna-Hensel, S. F. (2007). Preface. In M. D. Cavelty, V. Mauer & S. F. Krishna-Hensel (Eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (pp. ix-xiv). Aldershot, UK: Ashgate.

Krol, E., & Hoffman, E. (1993). FYI on "What is the Internet?" *Request for Comments, 1462 (FYI 20)*.

Kummer, M. (2005). Introduction. In W. J. Drake (Ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (pp. 1-6). New York: United Nations Information and Communications Technologies Task Force.

Laclau, E., & Mouffe, C. (1985). *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso.

Lake, D. (1999). Global Governance: A Relational Contracting Approach. In A. Prakash & J. A. Hart (Eds.), *Globalization and Governance* (pp. 31-53). London and New York: Routledge.

Lakoff, G., & Johnson, M. (1980). *Metaphors We Live By*. Chicago: University of Chicago Press.

Lakoff, G., & Johnson, M. (1989). *More Than Cool Reason*. Chicago: University of Chicago Press.

Larner, W., & Walters, W. (2004a). *Global Governmentality*. London and New York: Routledge.

Larner, W., & Walters, W. (2004b). Global governmentality: governing international spaces. In W. Larner & W. Walters (Eds.), *Global governmentality* (pp. 1-17). London: Routledge.

Larner, W., & Walters, W. (2004c). Globalization as governmentality. *Alternatives: Global, Local, Political, 29*(5), 495-515.

Latham, R. (2003). Introduction. In R. Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (pp. 1-24). New York: Social Science Research Council.

Latham, R. (2005). Networks, Information, and the Rise of the Global Internet. In R. Latham & S. Sassen (Eds.), *Digital Formations: IT and New Architectures in the Global Realm* (pp. 146-177). Princeton: Princeton University Press.

Latour, B. (1987). *Science in Action*. Cambridge, MA: Harvard University Press.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Levitsky, M. (2003). The dark side of globalization. *International Studies Review, 5*(2), 253-254.

Lewis, W. (1949). *America and Cosmic Man*. Garden City, New York: Double Day and Company Inc.

Lichtblau, E. (2008a). Congress Strikes Deal to Overhaul Wiretap Law [Electronic Version]. *New York Times*, 20 June. Retrieved 20 June 2008 from http://www.nytimes.com/2008/06/20/washington/20fisa.html?scp=1&sq=Congress%20Strikes%20Deal%20to%20Overhaul%20Wiretap%20Law&st=cse.

Lichtblau, E. (2008b). Senate Approves Bill to Broaden Wiretap Powers [Electronic Version]. *New York Times*, 10 July. Retrieved 10 July 2008 from http://www.nytimes.com/2008/07/10/washington/10fisa.html?_r=1&scp=1&sq=Senate%20Approves%20Bill%20to%20Broaden%20Wiretap%20Powers&st=cse&oref=slogin.

Licklider, J. C. R. (1960). Man-Computer Symbiosis. *IRE Transactions of Human Factors in Electronics, HFE-1*(1), 4-11.

Licklider, J. C. R. (1963). Memorandum for Members and Affiliates of the Intergalactic Computer Network: Topics for Discussion at Forthcoming Meeting (Advanced Research Projects Agency). Retrieved 3 March 2008, from http://packet.cc/files/memo.html

Licklider, J. C. R., & Taylor, R. (1968). Computer as Communications Device. *Science and Technology*(April).

Lieberman, J. (2008a). Letter to Eric Schmidt, Chairman of the Board and Chief Executive Officer, Google, Inc., from http://lieberman.senate.gov/newsroom/release.cfm?id=298006

Lieberman, J. (2008b). LETTER; Terror and the Internet: Senator Lieberman Responds [Electronic Version]. *New York Times*, 29 May from

http://query.nytimes.com/gst/fullpage.html?res=9F07E4DB1031F93BA15756C0A96E9C8B63&scp=2&sq=Lieberman%20YouTube&st=cse.

Linklater, A. (1998). *The Transformation of Political Community: Ethical Foundations for a Post-Westphalian Era*. Columbia, SC: University of South Carolina Press.

Lipschutz, R. D. (1992). Reconstructing World Politics: The Emergence of Global Civil Society. *Millennium: Journal of International Studies, 21*(3), 389-420.

Locke, J. (1988). *Two Treatises on Government*. Cambridge: Cambridge University Press.

Locke, J. (1998). *An essay concerning human understanding*. London and New York: Penguin.

Lovelock, J. E. (1987). *GAIA: A new look at life on Earth*. Oxford and New York: Oxford University Press.

Luke, T. (2004). Megametaphorics: Re-Reading Globalization and Virtualization as Rhetorics of World Politics. In F. A. Beer & C. l. De Landtsheer (Eds.), *Metaphorical World Politics* (pp. 217-236). East Lansing, MI: Michigan State University Press.

Lyon, D. (2003). *Surveillance after September 11*. Cambridge: Polity.

Macdonald, N. (2007). What happened to the 'war on terror' [Electronic Version]. *CBC News: Reports from Abroad*. Retrieved 13 September 2007 from http://www.cbc.ca/news/reportsfromabroad/macdonald/20070911.html.

Mackenzie, A. (2005). Problematising the Technological: The Object as Event. *Social Epistemology, 19*(4), 381-399.

MacLean, D. (2004). Herding Schrödinger's Cats: Some Conceptual Tools for Thinking about Internet Governance. In D. MacLean (Ed.), *Internet Governance: A Grand Collaboration* (pp. 73-100). New York: United Nations ICT Task Force.

MacLeish, A. (1968, 25 December 2008). A Reflection: Riders on the Earth Together, Brothers in Eternal Cold. *New York Times,* p. 1.

Maher, D. (2006). *Reporting to God*. Retrieved 5 October 2006, from http://chilit.org/Papers%20by%20author/Maher%20--%20Reporting%20to%20God.htm.

Malkin, G. (1993). The Tao of the IETF: A Guide for New Attendees of the Internet Engineering Task Force. *RFC 1391*.

Malkin, L., & Elizur, Y. (2001). The Dilemma of Dirty Money. *World Policy Journal, 18*(1), 13-23.

Mandaville, P. (1999). Territory and Translocality: Discrepant Idioms of Political Identity. *Millennium: Journal of International Studies, 28*(3), 653-673.

Margherio, L. (1998). *The Emerging Digital Economy*. Retrieved 26 January 2006. from http://www.technology.gov/digeconomy/emerging.htm.

Marshall McLuhan Foresees The Global Village. Retrieved 6 June 2007, from http://www.livinginternet.com/i/ii_mcluhan.htm

Mathiason, J. (2007). Internet Governance War: The Realists Strike Back. *International studies Review, 9*, 152-155.

Mathiason, J. (2008). *Internet Governance: The new frontier of global institutions*. New York: Routledge.

McCullagh, D. (2006). Terrorism invoked in ISP snooping proposal [Electronic Version]. *CNET News.com*. Retrieved 3 April 2008 from http://www.news.com/2102-1028_3-6078229.html

McGrew, A. (Ed.). (1997). *The Transformation of Democracy*. Cambridge/Milton Keynes: Polity/Open University Press.

McLuhan, M. (1962). *The Gutenberg galaxy : the making of typographic man*. Toronto: University of Toronto Press.

McLuhan, M. (1994). *Understanding Media: The Extensions of Man*. Cambridge, MA and London: MIT Press.

McPherson, T. (2006). Reload: Liveness, Mobility and the Web. In W. H. K. Chun & T. Keenan (Eds.), *new media/old media* (pp. 199-209). New York and London: Routledge.

McTaggart, C. (2004). *The Internet's self-governance gap: Law, markets, code, and norms as institutions of self-governance in the Internet operational community*. University of Toronto, Toronto.

MEPs back contested telecoms plan [Electronic (2008). Version]. *BBC News*, 08 July. Retrieved 08 July 2008 from http://news.bbc.co.uk/2/hi/technology/7495085.stm.

Millar, S. (2003). Blunkett revives plan to let agencies trawl phone and net users' records [Electronic Version]. *The Guardian*, http://www.guardian.co.uk/technology/2003/sep/2013/freespeech.politics/print Retrieved 13 March 2008.

Miller, P., & Rose, N. (1990). Governing economic life. *Economy and Society, 19*(1), 1-31.

Misa, P. (2004). *Leonardo to the Internet: Technology and Culture from the Renaissance to the Present*. Baltimore and London: John Hopkins University Press.

Mittleman, J. (2004). *Whither Globalization? The vortex of knowledge and ideology*. London and New York: Routledge.

Monohan, T. (Ed.). (2006). *Surveillance and Security: Technological Politics and Power in Everyday Life*. London and New York: Routledge.

Moran, J. (2005). State power in the war on terror: A comparative analysis of the UK and USA. *Crime, Law and Social Change, 44*, 335-259.

Morgenthau, H. J. (1948). *Politics Among Nations* (6th ed.). New York: Knopf.

Mosco, V. (2004). *The Digital Sublime: Myth, Power and Cyberspace*. Cambridge, MA: MIT Press.

Mueller, M. (2002). *Ruling the Root: Internet Governance and The Taming of Cyberspace*. Cambridge: MIT Press.

Mulholland, H. (2008). Government targets extremist websites [Electronic Version]. *Guardian*. Retrieved 15 April 2008.

Muppidi, H. (2004). *The Politics of the Global* Minneapolis and London: University of Minnesota Press.

Murphy, A. B. (1996). The sovereign state system as political-territorial ideal: historical and contemporary considerations. In T. J. Biersteker & C. Weber (Eds.), *State Sovereignty as Social Construct* (pp. 81-121). Cambridge: Cambridge University Press.

Musolff, A. (2004). *Metaphor and Political Discourse: Analogical Reasoning in Debates about Europe*. Basingstoke: Palgrave.

Näsström, S. (2003). What globalization overshadows. *Political Theory, 31*(6), 808-834.

National Science Foundation, & Harvard Information Infrastructure Project. (1995). Minutes: "Internet Names, Numbers, and Beyond: Issues in the Coordination, Privatization, and Internationalization of the Internet". Retrieved 15 August 2007, from

http://web.archive.org/web/20030226091340/http://www.ksg.harvard.edu/iip/GIIconf/nsfmin1.html

National Telecommunications Information Authority. (1998a). *A Proposal to Improve Technical Management of Internet Names and Addresses (Green Paper)*. Retrieved 20 January 2007. from http://www.ntia.gov/ntiahome/domainname/dnsdraft.htm.

National Telecommunications Information Authority. (1998b). Improvement of Technical Management of Internet Names and Addresses; Proposed Rule. *Federal Register, 63*(34), 8825-8833.

National Telecommunications Information Authority. (1998c). *Management of Internet Names and Addresses (White Paper)*. Retrieved 20 January 2007. from http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm.

Naughton, J. (2001). The Internet and Global Civil Society. In H. Anheiner, M. Galsius & M. Kaldor (Eds.), *Global Civil Society Yearbook 2001*. Oxford: Oxford University Press.

Nederman, C. J., & Forhan, K. L. (Eds.). (1993). *Medieval Political Theory - A Reader: The Quest for the Body Politic, 1100 - 1400*. New York and London: Routledge.

Negroponte, N. (1995). *Being Digital*. New York: Vintage Books.

New terror law comes into force [Electronic (2006). Version]. *BBC News*, 13 April. Retrieved 08 July 2008 from http://news.bbc.co.uk/2/hi/uk_news/politics/4905304.stm.

Nietzsche, F. (1911). On Truth and Falsity in an Ultramoral Sense (1873) (M. Mugge, Trans.). In F. Nietzsche (Ed.), *Early Greek Philosophy and other essays*. London: T.N. Foulis.

Nietzsche, F. (1989). *On the Genealogy of Morals and Ecce Homo* (W. Kaufmann & R. J. Hollingdale, Trans.). New York: Vintage Books.

Noble, G. W., & Ravenhill, J. (Eds.). (2000). *Asian Financial Crisis and the Architecture of Global Finance*. Cambridge: Cambridge University Press.

Nogales, P. (1999). *Metaphorically Speaking*. Stanford: Center for the Study of Language and Information.

Nuttall, C. (1998). Can Icann do it on Wednesday? *BBC News* Retrieved 18 March 2008, from http://news.bbc.co.uk/2/hi/science/nature/220919.stm

Nye, J. (2004). *Power in the Global Information Age*. London and New York: Routledge.

O'Brien, R., Goetz, A. M., Scholte, J. A., & Williams, M. (2000). *Contesting Global Governance: Multilateral Economic Institutions and Global Social Movements*. Cambridge: Cambridge University Press.

O'Neill, J. (1990). An Interview with Paul Baran. *Oral History* Retrieved 2 June 2007

O'Neill, O. (1986). *Faces of Hunger: An Essay on Poverty, Justice and Development*. London: Allen and Unwin.

Office of the Inspector General. (1993). *Review of NSFNET*. Washington: National Science Foundation.

Ohmae, K. (1990). *The Borderless World*. London: Collins.

Ohmae, K. (1995). *The End of the Nation State*. New York: Free Press.

Onuf, N. (1989). *A World of Our Making*: University of South Carolina Press.

OpenNet Initiative. (2007). Blog: EU interior ministers discuss on proposals to sanction or block Web sites (9 October). Retrieved 17 October 2007, from http://opennet.net/blog/?p=182

Pauly, L. W. (2002). Global Finance, political authority, and the problem of legitimation. In R. B. Hall & T. J. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 76-91). Cambridge: Cambridge University Press.

Pauly, L. W., & Grande, E. (Eds.). (2005). *Complex Sovereignty*. Toronto: University of Toronto Press.

Pemberton, J.-A. (2001). *Global Metaphors*. London: Pluto Books.

Pieterse, J. N. (2004). Neoliberal Empire. *Theory, Culture and Society, 21*(3), 119-140.

Plato. (1992). *Republic* (G. M. A. Grube, Trans.). Indianapolis and Cambridge: Hackett Publishing Company.

Poole, H., Schuyler, T., Senft, T. M., & Moschovitis, C. J. P. (1999). *History of the Internet - A Chronology, 1842-Present*. Oxford: ABC-CLIO.

Porter, T. (2005). *Globalization and Finance*. Cambridge: Polity Press.

Postel, J. (1996). New Registries and the Delegation of International Top Level Domains (draft RFC). Retrieved 25 October 2007, from http://tools.ietf.org/html/draft-postel-iana-itld-admin-00

Poulsen, K. (2005). FBI Retires Carnivore [Electronic Version]. *The Register*. Retrieved 4 April 2008 from http://www.theregister.co.uk/2005/01/15/fbi_retires_carnivore/.

Prakash, A., & Hart, J. A. (1999). *Globalization and Governance*. London: Routledge.

Presidential Directive on Electronic Commerce. (1997). Retrieved. from http://www.technology.gov/digeconomy/presiden.htm.

Quittner, J. (1994). Billions Registered [Electronic Version]. *Wired*, 2.10. Retrieved 27 July 2006 from

http://web.archive.org/web/19961128172624/www.wired.com/wired/2.10/departments/electrosphere/mcdonalds.html.

Quittner, J. (1996). Billions Covered [Electronic Version]. *Wired*, 2.10. Retrieved 27 July 2006 from http://web.archive.org/web/19961128172624/www.wired.com/wired/2.10/departments/electrosphere/mcdonalds.html.

Raban, J. (2005). The Truth About Terrorism. *The New York Review of Book, 52*(1).

Ramachander, S. (2008). Internet Filtering in Europe. In R. J. Deibert, J. Palfrey, R. Rohonzinski & J. Zittrain (Eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (pp. 186-196). Cambridge, MA: MIT Press.

Randall, N. (1997). *The Soul of the Internet*. London: International Thompson Computer Press.

Rasmussen, C., & Brown, M. (2005). The Body Politic as Spatial Metaphor. *Citizenship Studies, 9*(5), 469-484.

Read, J. (2006). Axes of Projection: Urbanization, Globalization, and Poetics in Latin America (pp. 30): University of Buffalo.

Rheingold, H. (1994). *The Virtual Community*. London: Martin Secker and Warburg.

Richard, M. M. (2005). *Prepared Statement of Mark M Richard - Presented at the Meeting of EU's Article 29 Working Group, Brussels 14 April 2005*. Retrieved 3 April 2008. from http://www.usdoj.gov/criminal/cybercrime/mmrArt29DRstmt041405.pdf.

Richards, I. A. (1981). The Philosophy of Rhetoric: Lecture V-Metaphor. In M. Johnson (Ed.), *Philosophical Perspectives on Metaphor* (pp. 48-62). Minnesota: University of Minnesota Press.

Richardson, M. (1996, 11 November). Staking Out 'Classy' Real Estate in Cyberspace. *International Herald Tribute*.

Ricoeur, P. (1977). *The Rule of Metaphor: Multi-disciplinary studies of creation of meaning in language*. Toronto: University of Toronto.

Ringmar, E. (1996). The ontological status of the state. *European Journal of International Relations, 2*(4), 439-466.

Risen, J. (2007). Subpoenas Sent to White House on Wiretapping [Electronic Version]. *New York Times*, 28 June. Retrieved 16 April 2008 from http://query.nytimes.com/gst/fullpage.html?res=9C00E0DB163EF93BA15755C0A9619C8B63&scp=2&sq=Subpoenas%20Sent%20to%20White%20House%20on%20Wiretapping&st=cse.

Risen, J., & Lichtblau, E. (2005). Bush Lets U.S. Spy on Callers Without Courts [Electronic Version]. *New York Times*, 15 December. Retrieved 16 August 2006 from http://www.nytimes.com/2005/12/16/politics/16program.html?_r=1&scp=11&sq=NSA+Wiretapping&st=nyt&oref=slogin.

Rorty, R. (1987). Hesse and Davidson on Metaphor. *Proceedings of the Aristotelian Society, Supplementary Volume*(LXI), 283-296.

Rorty, R. (1989). *Contingency, irony and solidarity*. Cambridge: Cambridge University Press.

Rorty, R. (1991). *Objectivity, relativism and truth*. Cambridge: Cambridge University Press.

Rose, N., & Miller, P. (1992). Political Power beyond the State: Problematics of Government. *The British Journal of Sociology, 43*(2), 173-205.

Rosenau, J. N. (2003). *Distant Proximities: Dynamics Beyond Globalization*. Princeton: Princeton University Press.

Rosenau, J. N. (2007). *People Count! Networked Individuals in Global Politics*. Boulder, CO: Paradigm Publishers.

Rosenau, J. N., & Czempiel, E.-O. (Eds.). (1992). *Governance without Government: Order and Change in World Politics*. Cambridge: Cambridge University Press.

Rosenau, J. N., & Singh, J. P. (Eds.). (2002). *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany: SUNY.

Rosenberg, J. (2000). *The Follies of Globalization Theory*. New York and London: Verso.

Rosenberg, J. (2005). Globalization Theory: A Post Mortem. *International Politics, 42*(1), 2-74.

Ruggie, J. G. (1993). Territoriality and beyond: problematizing modernity in international relations. *International Organization, 41*(1), 139-174.

Russell, A. (2005). Don't mention war on terror, say Bush aides [Electronic Version]. *The Telegraph*. Retrieved 20 November 2007 from http://www.telegraph.co.uk/core/Content/displayprintable.jhtml?xml=news/2--5/07/27/wterr27.xml&site=5&page=0.

Russell, A. L. (2006). 'Rough Consensus and Running Code' and the Internet-OSI Standards War. *IEEE Annals of the History of Computing, July/September*, 48-61.

Ryan, J. (2007). EU must take it anti-terrorism fight to the Internet. Retrieved 19 June 2008, from http://www.iiea.com/articlextext/php?article_id=23

Sack, R. D. (1986). *Human Territoriality: Its Theory and History*. Cambridge: Cambridge University Press.

Saco, D. (1999). Colonizing Cyberspace: "National Security" and the Internet. In J. Weldes, M. Laffey, H. Gusterson & R. Duvall (Eds.), *Cultures of Insecurity: States, Communities, and the Production of Danger* (pp. 261-291). Minneapolis: University of Minnesota Press.

Sageman, M. (2008). The Next Generation Terror. *Foreign Policy*(Mar/Apr), 37-42.

Saliban, J., & Sykes, J. (2002). UK Anti-Terrorism Act 2001 and ISP's: A Cyber Check-Point Charlie? *Computer, Law and Security Report, 18*(5), 338-339.

Sassen, S. (2000). Digital Networks and the State: Some Governance Questions. *Theory, Culture and Society, 17*(4), 19-34.

Sassen, S. (2001). Spatialities and Temporalities of the Global: Elements for Theorization. In A. Appadurai (Ed.), *Globalization* (pp. 260-278). Durham, NC: Duke University Press.

Sassen, S. (2006). *Territory, Authority, Rights*. Princeton: Princeton University Press.

Schmitt, E., & Shanker, T. (2008). U.S. Adapts Cold-War Idea to Fight Terrorists [Electronic Version]. *New York Times* from http://www.nytimes.com/2008/03/18/washington/18terror.html?scp=1&sq=U.S.+Adapts+Cold+War+Idea+to+Fight+Terrorists&st=nyt.

Scholte, J. A. (2000). *Globalization: A Critical Introduction* (1st ed.). New York: Palgrave.

Scholte, J. A. (2005). *Globalization: A Critical Introduction* (2nd ed.). Basingstoke and New York: Palgrave.

Scholte, J. A. (2008). Preface. In M. Kornprobst, V. Pouliot, N. Shah & R. Zaiotti (Eds.), *Metaphors of Globalization: Mirrors, Magicians and Mutinies* (pp. ix-x). Basingstoke: Palgrave.

Scholte, J. A. (forthcoming). *Civil Society and Global Democracy*. Cambridge: Polity

Scrap data retention plans, say MPs [Electronic (2003). Version]. *ZDNet.co.uk*. Retrieved 2 April 2008 from http://www.zdnet.co.uk/misc/print/0,1000000169,2129559-39001084,00.htm.

Seamon, R. H., & Gardner, W. D. (2005). The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement. *Harvard Journal of Law and Public Policy 28*(2), 319-463.

Searle, J. R. (1981). Metaphor. In M. Johnson (Ed.), *Philosophical Perspectives on Metaphor* (pp. 248-285). Minneapolis: University of Minnesota Press.

Semino, E., & Culpeper, J. (Eds.). (2002). *Cognitive Stylistics: Language and Cognition in Text Analysis*. Amsterdam: John Benjamins.

Sending, O. J., & Neumann, I. B. (2006). Governance to Governmentality: Analyzing NGOs, States and Power. *International Studies Quarterly, 50*(3), 651-672.

Shah, N. (2006). Cosmopolitanizing and Decosmopolitanizing Globalization: Metaphorical Re-description and Transformations of Political Community. *Globalizations, 3*(3), 393-411.

Sims, S., & Walker, D. (2003). *The Discourse of Sovereignty, Hobbes to Fielding: The State of Nature and the Nature of the State* Hampshire: Ashgate.

Skinner, Q. (1978). *The Foundations of Modern Political Thought: The Age of Reformation* (Vol. 2). Cambridge University Press: Cambridge University Press.

Skinner, Q. (1989). The state. In T. Ball, J. Farr & R. L. Hanson (Eds.), *Political Innovation and Conceptual Change* (pp. 90-131). Cambridge: Cambridge University Press.

Slaughter, A.-M. (2004). *A New World Order*. Princeton: Princeton University Press.

Smith, M. S., Seifert, J. W., McLoughlin, G. J., & Moteff, J. D. (2002). The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government. *CRS Report for Congress*(4 March).

Smith, N. (2005). *The Endgame of Globalization*. New York and London: Routledge.

Smith targets internet extremism [Electronic (2008). Version]. *BBC News*. Retrieved 2 April from http://news.bbc.co.uk/2/hi/uk_news/politics/7193049.stm.

Solove, D. J. (2003). Reconstructing Electronic Surveillance Law. *The George Washington Law Review, 27*(6), 1264-1305.

Sparke, M. (2006). A neoliberal nexus: Economy, security and the biopolitics of citizenship on the border. *Political Geography 25*(2), 151-180.

Sparke, M. (forthcoming). Unpacking economism and remapping the terrain of global health In O. Williams & A. Kay (Eds.), *Global Health Governance: Transformations, Challenges and Opportunities Amidst Globalization*. London: Palgrave.

Spruyt, H. (1994). *The Sovereign State and Its Competitors*. Princeton, NJ: Princeton University Press.

Steffek, J. (2003). The Legitimation of International Governance: A Discourse Approach. *European Journal of International Relations, 9*(2), 249-275.

Stefik, M. (Ed.). (1996). *Internet Dreams: Archetypes, Myths and Metaphors*. Cambridge, MA: MIT Press.

Steger, M. (2003). *Globalization: A Very Short Introduction*. Oxford and New York: Oxford University Press.

Steger, M. (2004). Introduction: Rethinking the Ideological Dimensions of Globalization. In M. Steger (Ed.), *Rethinking Globalism* (pp. 1-14). Lanham: Rowman and Littlefield.

Steger, M. (2005). From Market Globalism to Imperial Globalism: Ideology and American Power after 9/11. *Globalizations, 2*(1), 31-46.

Steger, M. (2006). Imperial Globalism, Democracy and the 'Political' Turn. *Political Theory, 34*(3), 372-382.

Steger, M. (2008). *The Rise of the Global Imaginary*. New York: Oxford University Press.

Stiglitz, J. (1999). Reforming the Global Financial Architecture: Lessons from the Recent Crises. *Journal of Finance, 54*(4), 1508-1521.

Stilkind, J. (1996). The Internet: Creating a Democratic Global Village. *USIA: Global Issues, 12*(1).

Strange, S. (1996). *The Retreat of the State*. Cambridge: Cambridge University Press.

Strange, S. (1998). Globaloney. *Review of International Political Economy, 5*(4), 704-720.

Tarrow, S. (2005). *The New Transnational Activism*. Cambridge: Cambridge University Press.

Tedeschi, B. (2003). Patriot Act Curbing Data Retention [Electronic Version]. *New York Times*, 13 October. Retrieved 3 April 2008.

The 2nd Boston Tea Party. (2000). Retrieved 07 July 2007, from http://web.archive.org/web/20030422195610/http://www2.aus.us.mids.org/mn/1007/tea.html

Thompson, J. E., & Krasner, S. (1989). Global Transactions and the Consolidation of Sovereignty. In E.-O. Czempiel & J. N. Rosenau (Eds.), *Global Changes and Theoretical Challenges*. Lexington, MA and Toronto: Lexington Books.

Townsend, M. (2006). Leak reveals official story of London bombings [Electronic Version]. *The Guardian*. Retrieved 11 November 2007 from http://www.guardian.co.uk/uk/2006/apr/09/july7.uksecurity.

Travis, A. (2008). Whitehall draws up new rules on language of terror [Electronic Version]. *The Guardian* from //www.guardian.co.uk/politics/2008/feb/04/uk.terrorism.

Troyer, L. (2002). The Calling of Counterterrorism. *Theory and Event, 5*(4), no pagination.

Turner, F. (2006). *From Counterculture to Cyberculture: Steward Brand, The Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

U.S. Department of Commerce, & Internet Corporation for Assigned Names and Numbers. (1998). Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. from www.icann.org/general/icann-mou-25nov98.htm

U.S. Government. (2001). The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Retrieved 10 October 2008, from http://thomas.loc.gov/cgi-bin/query/D?c107:4:./temp/~c107tbOsGt::

U.S. Government. (2002). The National Security Strategy of the United States of America. Washington, DC.

U.S. ISPA, & EuroISPA. (2002). EUROISPA and US ISPA Position on the Impact of Data Retention Laws on the Fight Against Cybercrime Retrieved 3 April 2008, from http://www.euroispa.org/docs/020930eurousispa_dretent.pdf

U.S. rejects Name plan [Electronic (1997). Version]. *CNET News.com* from http://web.archive.org/web/20000822082123/http://yahoo.cnet.com/news/0-1005-200-318681.html.

Ugelow, S. (1994). Address for Success: Internet Name Game; Individuals Snap Up Potentially Valuable Corporate E-mail IDs. *The Washington Post,* p. a01.

United Nations. (2003). World Summit on the Information Society - Geneva Declaration of Principles [Electronic Version]. *Document WSIS-03/GENEVA/DOC/4-E* Retrieved 25 October 2005 from http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

United States House of Representatives. (2007). Violent Radicalization and Homegrown Terrorism Prevention Act of 2007 [H.R. 1955]. Retrieved 6 July 2008, from http://www.govtrack.us/congress/billtext.xpd?bill=h110-1955

United States Senate Committee on Homeland Security and Governmental Affairs. (2008). Violent Islamist Extremism, the Internet and the Homegrown Terrorist Threat. Retrieved 6 July, 2008, from http://hsgac.senate.gov/public/_files/IslamistReport.pdf

US 'to end warrantless wiretaps' [Electronic (2007). Version]. *BBC News*, 17 January. Retrieved 11 July 2008.

US House passes surveillance law [Electronic (2008). Version]. *BBC News*, 15 March. Retrieved 11 July 2008 from http://news.bbc.co.uk/go/pr/fr/-/2/hi/americas/7297865.stm.

US ISPA. (2005). US ISPA Comments on the USA PATRIOT Act Sunset Provisions. Retrieved 2 April 2008, from http://www.cix.org/pdf/US_ISPA_Patriot_Act_Position_Paper.pdf

USC/ISI. (1999). 30 years of RFCs. *RFC 2555*.

Valovic, T. (2000). *Digital Mythologies: The Hidden Complexities of the Internet*. New Brunswick, NJ and London: Rutgers University Press.

Vincent, J. (1974). *Non-intervention and International Order*. Princeton: Princeton University Press.

Wakefield, J. (2007). Confusion over 'data snooping' laws [Electronic Version]. *BBC News*. Retrieved 2 April 2008 from http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6358779.stm.

Walker, R. B. J. (1993). *Inside/Outside: International Relations as Political Theory*. Cambridge: Cambridge University Press.

Walker, R. B. J. (1997). The Subject of Security. In K. Krause & M. C. Williams (Eds.), *Critical Security Studies: Concepts and Cases* (pp. 61-83). London: UCL Press Limited.

Walker, R. B. J. (2003). Polis, cosmopolis, politics. *Alternatives: Global, Local, Political, 28*(2), 267-286.

Waltz, K. N. (1959). *Man, the State and War*. New York: Columbia University Press.

Waltz, K. N. (1979). *Theory of International Politics*. Boston: McGraw-Hill.

Ward, B. (1966). *Spaceship Earth*. New York: Columbia University Press.

Watson, S. (2006). 7/7 Reports: You will lose your privacy but next attacks can't be prevented [Electronic Version]. *Infowars.net*. Retrieved 22 November 2007 from http://www.infowars.net/articles/may2006/120506bombings.htm.

Weber, C. (1995). *Simulating Sovereignty: Intervention, the state and symbolic exchange*. Cambridge: Cambridge University Press.

Weber, C. (2002). Flying Planes Can Be Dangerous. *Millennium: Journal of International Studies, 31*(1), 129-148.

Webster, F. (2006). *Theories of the Information Society* (3rd ed.). London and New York: Routledge.

Weiss, L. (1998). *Myth of the Powerless State*. Ithaca: Cornell University Press.

Wellman, B., & Haythornthwaite, C. (Eds.). (2002). *The Internet in Everyday Life*. Oxford: Blackwell Publishing.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Whitaker, R. (2001). The Dark Side of Life: Globalization and International Organized Crime. In R. Whitaker (Ed.), *A World of Contradictions* (pp. 1-15). London: Merlin.

Winner, L. (1997). Cyberlibertarians Myths and the Prospects for Community [Electronic Version] from http://www.rpi.edu/~winner/cyberlib2.html.

Wolf, M. (2001). Why this Hatred of the Market? In F. J. Lechner & J. Boli (Eds.), *The Globalization Reader* (pp. 9-11). Oxford: Blackwell Publishers.

Wolin, S. (1993). Reason in Exile: Critical Theory and Technological Society. In A. M. Melzer, J. Weinberger & M. R. Zinman (Eds.), *Technology and the Western Political Traditional* (pp. 162-189). London and Ithaca, NY: Cornell University Press.

Wong, M. W. (2002). Electronic Surveillance and Privacy in the United States after September 11 2001: The USA PATRIOT Act. *Singapore Journal of Legal Studies*(1), 214-270.

Woods, N. (1999). Good Governance in International Institutions. *Global Governance, 5*(1), 39-61.

Woods, N. (2006). *The Globalizers: The IMF, the World Bank and Their Borrowers*. Ithaca: Cornell University Press.

Working Group on Preventing Violent Extremism. (2005). Working Together to Prevent Violent Extremism (Working Group Report). Retrieved 05 July 2008, from http://www.communities.gov.uk/documents/communities/pdf/152164.pdf