Harvard Journal of Law & Technology
Volume 10, Number 3 Summer 1997

CYBERSPACE SOVEREIGNTY? — THE INTERNET AND THE INTERNATIONAL SYSTEM

Timothy S. Wu[*]

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*[1]

> *By linking with the Internet, we don't mean absolute freedom of information. I think there is a general understanding about this. If you go through customs, you have to show your passport. It's the same with management of information. There is no contradiction at all between the development of telecommunications infrastructure and the exercise of state sovereignty.*[2]

Will cyberspace exercise its own sovereignty? Does it do so already?

TABLE OF CONTENTS

---

* J.D., Harvard Law School, Class of 1998. The author would like to acknowledge the help of Lawrence Lessig and Anne-Marie Slaughter in the preparation of this Note. In addition, the author is thankful for helpful discussions with John Perry Barlow, Jonathan Yong-Sung Kang, Fernanda Lai, Quaid Morris, Richard A. Posner, George Wang, Jonathan Zittrain, and the participants in the Seminar on Law & Cyberspace taught by Professor Lessig at Harvard Law School.

1. John Perry Barlow, *A Declaration of the Independence of Cyberspace* (visited Feb. 13, 1997) <http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration>.

2. *Much of the Information Highway Still to Be Paved*, THE STRAITS TIMES, Nov. 25, 1995, at L1 (quoting Wu Jichuan, Minister of Posts and Telecommunications, People's Republic of China).

I. INTRODUCTION

There is no shortage of discussion concerning the operation of law in cyberspace. Some writers conclude that regulating cyberspace is really nothing new; others argue that cyberspace ought not to be regulated, or is impossible to regulate.[3] Certain exponents of the latter view have approached the question more broadly, asserting that cyberspace does or should enjoy a kind of international sovereignty. Probably the most outspoken advocates of "cyberspace sovereignty," as this idea is called, are the Electronic Frontier Foundation ("EFF")[4] and *Wired* magazine. David Johnson and David Post — both associated with the EFF — have recently presented a comprehensive argument for cyberspace sovereignty.[5]

Proponents of cyberspace sovereignty usually present a normative argument — that nations *should* respect the rules of cyberspace.[6] However they often make a descriptive, or predictive, statement as well: they claim that the "territorial" powers of the world *will*, or already *do*, respect an emergent cyberspace sovereignty. Such writers generally

3. *See, e.g.*, Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1744 (1995); John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207 (1997).

4. The Electronic Frontier Foundation is probably the best known and best funded organization advocating the freedom of the Internet and other technologies from government regulation. *See generally The Electronic Frontier Foundation* <http://www.eff.org>.

5. *See* David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996). David Johnson is a former chairman of the EFF, and David Post is a Policy Fellow of the EFF. Both are co-directors of the Cyberspace Law Institute. *See Cyberspace Law Institute* <http://www.cli.org>.

6. *See, e.g.*, Johnson & Post, *supra* note 5, at 1391-95.

assert that state regulation of the Internet will be impossible or futile. If this assertion is correct, cyberspace sovereignty will be a reality. Moreover, it could be the case that states will simply choose, for self-interested reasons, not to regulate cyberspace.

This Note examines two related questions: First, is it possible for nation states to regulate the Internet? Second, assuming that it is possible, will nation states regulate the Internet? Part II addresses the first question, arguing that Johnson and Post's descriptive assumptions are incorrect, and that Internet regulation, although difficult, is possible and stands to become increasingly so regardless of its desirability on normative grounds.[7] Parts III and IV address the second question: to what extent will states choose to regulate cyberspace? To answer this question we turn to models of state behavior in international relations theory. Part III examines cyberspace under an institutionalist framework, borrowing a set of assumptions identified with the realist theory of international relations. On this theory, which regards the international system as a homogenous community of power-maximizing actors, cyberspace sovereignty will be very narrow and largely defined by collective interest at the state level. Part III also examines some problems with the realist assumptions in the Internet context, and leads to the conclusion that the liberal theory of international relations may be more applicable. Part IV examines Internet regulation under that theory. The conclusion is that, under the assumptions of the liberal theory, the promulgation of widely acceptable cyberspace standards and norms may lead first individuals, and then states, to reach a consensus regarding what can be termed a "minimally sovereign" cyberspace.

II. THE FEASIBILITY OF CYBERSPACE REGULATION

Proponents of cyberspace sovereignty generally assert that it is impossible or futile for governments to regulate the Internet. In the words of John Perry Barlow: "I declare the global social space we are building to be naturally independent of the tyrannies you [the governments] seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."[8] Two varieties of Internet regulation must be considered here. Under the first, content regulation, the state controls the access of its citizens to the

---

7. There may also be good reason to question the normative arguments made by Johnson and Post. For a criticism of these arguments, especially the argument that the "effects" of actions in cyberspace are not geographically based, see Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1407-10 (1996).

8. Barlow, *supra* note 1.

materials available in cyberspace. Under the second, activity regulation, the state controls the actions that take place in or through cyberspace.

A. Content Regulation

Canvassing several different forms of government content regulation, Johnson and Post conclude that each is impracticable or impossible.[9] They are correct that *perfect* regulation of content is impossible, and that the Internet does make regulation especially difficult. But where the state can raise the costs of accessing forbidden content to a sufficient level, it can effectively deter most users from receiving undesired content. Often, the best way for states to do this is to implement or require changes in the hardware and software that allow cyberspace to exist. Several commentators note that governments have begun to regulate the software and hardware of the Internet.[10] Such regulation represents a profound shift in government responses to the Internet, and one that may prove especially effective.[11] At present, and to varying degrees, many states seem to have the power to do this. The following analysis will consider hardware- and software-based regulation, and then describe some actual attempts by nation states to implement this kind of regulation.

---

9. *See* Johnson & Post, *supra* note 5, at 1370-76. The descriptive claims in *Law and Borders* seem more extreme than any made elsewhere by either author. For example, Johnson has written that "even those who might go the extreme with such a view, perhaps advocating 'sovereignty' for the net, nevertheless must recognize that plodding old territorial sovereigns will continue to assert jurisdiction and make [law] about what happens online." David R. Johnson, *Jurisdictional Quid Pro Quo and the Law of Cyberspace* <http://www.eff.org/pub/Publications/David_Johnson/>. Similarly, the "evolutionary" approach to the cyberspace rule set advocated elsewhere by Post rests on a weaker descriptive claim that government regulation will be futile. *See* David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3 <http://www.law.cornell.edu/jol/post.html>.

10. "Hardware regulation" refers to control over the physical components of the network — for example, controlling what is connected to what. "Software regulation" refers to government control over the computer programs used to manage information. This distinction is not airtight: many functions can be implemented equally well using software or hardware.

11. That regulation by code is especially effective does not mean that it is necessarily good or bad. Cyberspace has been described as a "software world" where the "code is the law." *See, e.g.*, M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. LEGAL F. 335 (1996). However, it seems equally true that cyberspace is a hardware world. For the relevance of this for government regulation of the Internet, see, e.g., Lessig, *supra* note 7, at 1408.

1. Regulation via Hardware

Johnson and Post assert that because "individual electrons can easily, and without any realistic prospect of detection, 'enter' any sovereign's territory," controlling the flow of electronic information across borders is impossible.[12] It is not clear, however, how this conclusion follows from the premise. First of all, at least for the Internet, electrons are not the relevant unit — Internet Protocol ("IP") packets are. And in order for IP packets to enter a particular territory, certain physical components must be present there. By exercising control over the physical components required for Internet access, the state can regulate cyberspace.

At the most basic level, a state can simply choose not to have any connection to the Internet. Of course this means that the state must forego the considerable benefits of Internet communications, including electronic commerce and the increased prosperity it may bring.[13] Nevertheless, states that fear for their ability to regulate the Internet could choose this option. As of July 1996, at least thirty-three states were completely unconnected.[14] At another level, the state can compel the creation of a hierarchical network and then impose control over the top level router in that hierarchy (the gateway host).[15] By controlling the gateway to a subnet,[16] the state can regulate the Internet in its territory. It does not seem relevant whether government control of the gateway components is direct (the government owns the components) or indirect (the government regulates Internet service providers). The point is that where widespread usage of the Internet depends on physical components, a government that controls these components can regulate cyberspace.

---

12. Johnson & Post, *supra* note 5, at 1372. Johnson and Post assert that this is true at least for countries that "hope to participate in global commerce." *Id.* There is a clear conflict between the desire to reap the economic benefits of the Internet on the one hand and the desire to regulate it on the other. This issue is considered more fully *infra* at note 54 and accompanying text. Note, however, that two of the countries considered here, China and Singapore, have effectively imposed regulation on the Internet yet still participate in the global economy. Johnson and Post also make implicit reference to a division in state attitudes to the Internet between Western and non-Western countries. For a discussion of relevance of regional attitudes for cyberspace sovereignty, see *infra* Part IV.

13. For a discussion of this cost-benefit calculation, see *infra* note 54 and accompanying text.

14. *See Editorial: State of the Internet, July 1996*, MATRIX MAPS Q., July 1996, at 3, *available at* <http://www3.mids.org/mmq/304/pubhtml/ed.html>.

15. The gateway host is the point of entry, or gate, through which all information must pass if it is to enter or leave the network. A router is a piece of hardware that sends incoming packets to their intended destinations, based on the addresses they bear.

16. A subnet is a network connected to the main network (here the entire Internet) at only one point (the gateway host).

Of course the barriers imposed by gateway servers may be overcome. First, the user can use normal telephone lines to dial up a provider outside the subnet in question. Second, the user can send or receive encrypted information. Because it is nearly impossible for the government to determine the content of encrypted messages, regulation of such content will be difficult. However, these "exit options" from state control are probably of such a high cost, financially or in terms of necessary expertise, as to render them marginal to the discussion.[17]

The best example of a country pursuing subnet-based regulation of the Internet is China. With the help of several United States companies, China has already built two major government-operated intranets connected to the rest of the Internet through a limited number of regulated servers.[18] The China Wide Web, a subnet that will connect all of China's major population centers and provide Chinese language content, is supposed to begin operation soon.[19] It too will have controlled contacts with the Internet.

2. Regulation via Software

Another form of content regulation discussed by Johnson and Post is the software barrier, which they predict "will likely fail as well."[20] But again, the evidence for this view seems slender. There are two loci where software regulation is most effective — at the router level and at the end user level. At the router level, Internet regulation is typically accomplished through use of a firewall, or comprehensive system of network filtration and control, implemented typically at a gateway router.[21] A major component of a firewall system is what is called a

---

17. *See* Joshua Gordon, *East Asian Censors Want to Net the Internet*, THE CHRISTIAN SCI. MONITOR, Nov. 12, 1996, at 19 ("Restrictions in China and Singapore now put the last source of uncensored news firmly out of the reach for all but the wealthiest and most dedicated Internet hackers in those countries.").

18. *See* Sheila Tefft, *China Attempts to Have Its Net and Censor It Too*, CHRISTIAN SCI. MONITOR, Aug. 5, 1996, at 1; Graham Hutchings, *Beijing Builds Barriers Against an Electronic Democracy Wall*, DAILY TELEGRAPH, Mar. 15, 1996 at 38; *China Has 100,000 Internet Subscribers*, XINHUA NEWS AGENCY, Jan. 24, 1997, *available in* LEXIS, News Library, Xinhua File.

19. *See Bay Networks to Provide Core for China Wide Web*, XINHUA NEWS AGENCY, Jan. 14, 1997, *available in* LEXIS, News Library, Xinhua File; Michael Laris, *The Price of the Deal*, NEWSWEEK, Dec. 9, 1996, at 44; Chris McCall, *China Goes Online a Bit with Limited-Access "Intranet,"* AGENCE FRANCE PRESSE, March 31, 1997, *available in* LEXIS, World Library, Allnws File.

20. Johnson & Post, *supra* note 5, at 1374.

21. *See* JOHN WACK & LISA CARNAHAN, KEEPING YOUR SITE COMFORTABLY SECURE: AN INTRODUCTION TO INTERNET FIREWALLS (National Inst. of Standards and Tech. Special Pub. No. 800-10, 1995), *available at* <http://csrc.ncsl.nist.gov/nistpubs/800-10/>. The Rotherwick Firewall Resource web site has a collection of "must read" papers. *See* Zeuros

packet filtration router. Such a router can filter out packets coming from or going to specific IP addresses. This allows the owner of the firewall system to prevent inside users from accessing outside sites, or vice versa.[22] Much of what is considered the "free" Internet at present is already privately regulated through the use of firewalls, typically by corporations.[23] There does not seem to be any intrinsic reason why nation states will "fail" using similar technology. As a part of the subnet system discussed above, China is presently investing considerable energy in the development of a "digital Great Wall of China"[24] for its intranets using firewall technology developed by or with the assistance of United States companies.[25] Singapore also relies on firewall technology, especially proxy servers.[26]

At the end-user level, the state can rely on what is called "end-user filtering software" to filter out content. Recently there has been enormous development in the sophistication of end-user filtration systems. Most significantly, wide adoption of the PICS protocol would allow both sensitive and thorough content filtration, at least for the World Wide Web.[27] Where every site is reliably PICS rated, private individuals using PICS compatible browsers can elect not to receive undesirable content based on several content variables, such as violence,

---

Network Solutions, *The "Must Reads"* <http://www.zeuros.co.uk/firewall/mustread.htm>.

22. Of course, actual firewall systems are more complicated than the simple packet filtration router system described here. A typical component is an application gateway that protects certain sites. If an outside or insider user wishes to access these sites with an application program, she must allow the gateway host itself to run the application using proxy software. In this way the host can monitor the purposes for which the application is being used, and filter any necessary content.

23. *See* John S. Quarterman & Smoot Carl-Mitchell, *What is the Internet, Anyway?*, MATRIX NEWS, August 1994, art. 1, *available at* <http:www3.mids.org/mn/2>. Note that the Internet may not be as pervasive an unregulated network as many assume, because so much of what is considered part of the Internet is firewalled off. *See id.*

24. Louise Kehoe, *A Tricky Decision: Eagle Eye*, FIN. TIMES, Dec. 18, 1996, at 14.

25. *See* Laris, *supra* note 19, at 44.

26. For a brief explanation of proxy servers, see *supra* note 22. For a more detailed analysis of the Singaporean system, see Peng Hwa Ang & Berlinda Nadarajan, *Censorship and the Internet: A Singaporean Perspective*, COMM. ACM, June 1996, at 72. More information on the Internet regulation scheme in Singapore is available at the Singapore Broadcasting Authority web site. *See SBA Safeguards Community Interest Through Internet Regulation* <http://www.sba.gov.sg/netreg/regrel.htm>.

27. The PICS protocol seems likely to become the new standard for Internet content labeling. As it becomes more pervasive, a consequence will likely be easier regulation of the World Wide Web by nation states. For a general overview, see Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, COMM. ACM, Oct. 1996, at 87, *available at* <http://www.w3.org/pub/WWW/PICS/iacwcv2.htm>; Paul Resnick, *Filtering Information on the Internet*, SCI. AM., Mar. 1997, at 62. *See also* Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. (forthcoming 1997), *available at* <http://www.msen.com/~weinberg/rating.htm>.

sex, and so forth. Theoretically, such screening can be done with complete accuracy.[28] End-user filtering software may also be used to facilitate state control over Internet content. For example, a state could require by law that all browsers made available in the country come equipped with filtration software. This regulation would be easier to avoid than router regulation, because the filtration program would be in the hands of end users. Furthermore, pirated browsers would likely proliferate.[29] Yet insofar as the bundled filtration software served to increase the costs of exit from the state's rule set, such regulation will be another means by which the state can effectively regulate cyberspace.

China and Singapore furnish the paradigm for effective cyberspace regulation. The point here is not that the regulation exercised by China and Singapore is perfect — of course it is not. What matters is that, by all accounts, these nations have been able to limit the activity of ordinary users.[30] So far these users have accepted the restrictions, or at least have not considered them worth complaining about.[31] It might be argued that China and Singapore are bizarre examples of Internet regulation, made uniquely possible only by a combination of limited Internet connections and a strong government. Or perhaps because so many Asian countries are planning to or already regulate the Internet, this can be considered a regional quirk.[32] Yet many of the descriptive claims for cyberspace sovereignty seem plausible only in the face of a highly decentralized network and a limited government. Such features are characteristic of Western liberal democracy in general, and American society in particular; in the world's nations they are absent. There is a reason, then, to

---

28. *See* Weinberg, *supra* note 27. At least in the United States, end-user Internet filtering software has been touted by free speech activists and Communications Decency Act litigators as an answer to government regulation of content. *See id.*

29. A state could deal with this problem to some extent by requiring users to register their browsers; the state could then check whether the browser were authorized before permitting the transfer of content.

30. *See supra* note 17 and accompanying text. Jeffrey Schiller makes the point that even ordinary users can quickly and easily gain access to the security-cracking tools of an expert. Jeffrey Schiller, Internet Rights Versus Internet Security, Talk Sponsored by the M.I.T. Technology and Culture Forum (Mar. 18, 1997). However, even getting these expert tools probably involves effort and learning beyond what ordinary users can be expected to undertake.

31. *See Opening Internet Roads into China; Software Giants Are Set to Provide Access, Undaunted by Threats of State Controls*, S.F. EXAMINER, Sept. 12, 1996, at B1 ("Service providers, which have proliferated in recent months, say that they have had few complaints from clients unable to access some sites and that enthusiasm for the Internet is undiminished."). This may of course change with time and exposure to the Internet.

32. *See* Gordan, *supra* note 17.

question the arguments for cyberspace sovereignty inasmuch as they seem to make sense only in particular contexts.[33]

B. Activity Regulation

Adherents of cyberspace sovereignty assert as well that regulation of activities pursued in or through cyberspace is futile. The basis for this claim is best laid out by David Post in *Anarchy, State, and the Internet: An Essay on Law Making in Cyberspace*.[34] There, Post emphasizes that the Internet represents a highly accessible "exit-option" from the territorial rule set. He offers two reasons. First, discovering illegal behavior is costly in a decentralized network. Second, local prohibitions on information and services (such as pornography) will lose their force where individuals can use the Internet to obtain such content from servers located in less restrictive jurisdictions.[35]

Or so they say. Yet mysteriously we find Robert and Carleen Thomas in federal prison,[36] joining a list of convicts that includes people like Bob Morris, Phiber Optik,[37] and an individual in Singapore who was subjected to massive fines for downloading pornographic material from the Internet.[38] Though it may be difficult, detecting illegal behavior on the Web is far from impossible. Naturally, the powerful search capabilities available in cyberspace help. And it is unclear that the difficulties of detection in cyberspace are any greater than those posed by many traditional kinds of illegal behavior.

The force of the second point — that illegal activities will seep in from other jurisdictions — seems limited. States can still go after any suppliers of illegal content who have contacts with the jurisdiction. If

---

33. The possibility that different states will entertain differing attitudes towards the Internet between states is treated below. *See infra* Part IV. For additional criticism of Johnson and Post's descriptive arguments, see Lessig, *supra* note 7, at 1404-06.

34. Post, *supra* note 9.

35. *See id.* ¶¶ 39-41.

36. Robert and Carleen Thomas were the operators of the Amateur Action BBS, a purveyor of sexually explicit GIF files. They were sentenced to 30 and 37 months in prison by a United States district court after a postal inspector in Tennessee downloaded GIF files from their BBS and reported them. *See* United States v. Thomas, 74 F.3d 701, 704-07 (6th Cir. 1996).

37. Bob Morris was convicted of using the Internet Worm, a program he had written, to obtain access to federal computers in violation of the Computer Fraud and Abuse Act of 1986 § 2(d), 18 U.S.C. § 1030(a)(5)(A) (1994). He was sentenced to three years of probation, 400 hours of community service, and a fine of $10,050. *See* United States v. Morris, 928 F.2d 504, 506 (2d Cir. 1991). Phiber Optik is a famous hacker who served over 10 months in prison; he was also sentenced to probation and 600 hours of community service. *See* Paula Span, *Modem Operandi: Phiber Optik, Bad Boy Hacker, Out of Stir and On-Line*, WASH. POST, Jan. 13, 1995, at B1.

38. *See* Gordan, *supra* note 17.

this kind of direct state regulation is avoidable at all, it will require physical relocation.[39] Many states have been and will be able to regulate behavior beyond their borders.[40] Though the ease of Internet communication does exacerbate the problem of foreign suppliers, states can always respond by turning to content regulation of the type discussed in the previous section.

Thus states do have the power to regulate the Internet; the interesting question becomes whether they will choose to do so. Answering this question requires an analysis of the international system, to which we now turn.

III. INSTITUTIONALIST THEORY AND THE INTERNET

One approach we might adopt in answering this question is the realist or institutionalist view of international regimes. One author has defined the concept of an international regime to comprehend "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue-area."[41] It may be useful to think of cyberspace as a kind of international regime. Under the institutionalist view, states will adhere to the rules of this regime if and only if it is in their rational interest to do so.[42]

---

39. An example is Playboy's trademark infringement action against the "Playmen" web site. *See* Playboy Enterprises v. Chuckleberry, 1996 U.S. Dist. LEXIS 8435 (S.D.N.Y. 1996); *see also* John T. Soma, *Transnational Extradition for Computer Crimes: Are new Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. (forthcoming 1997).

40. For example, the United States forced Panama's head of state, Manuel Noriega, to stand trial in Miami for drug-related charges. *See Noriega's Guilt, and Its Aftertaste*, N.Y. TIMES, Apr. 11, 1992, at 1, 24.

41. Stephen D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES 1, 2 (Stephen D. Krasner ed., 1983). Krasner defines principles as "beliefs of fact, causation, and rectitude," norms as "standards of behavior defined in terms of rights and obligations," rules as "specific prescriptions or proscriptions for action," and decision-making procedures as "prevailing practices for making and implementing collective choice." *Id.* Another definition of regimes is that of "governing arrangements" that include "networks of rules, norms, and procedures that regularize behavior and control its effects." ROBERT O. KEOHANE & JOSEPH S. NYE, POWER AND INTERDEPENDENCE 19 (1977). Professor Slaughter makes the point that in many respects, the development of regime theory was simply a rediscovery of international law. *See* Anne-Marie Slaughter Burley, *International Law and International Relations Theory: A Dual Agenda*, 87 AM. J. INT'L L. 205, 219-22 (1993).

42. *See generally* ROBERT O. KEOHANE, AFTER HEGEMONY: COOPERATION AND DISCORD IN THE WORLD POLITICAL ECONOMY (1984). For an overview of the developments leading to rationalist/institutionalist regime theory, see Slaughter Burley, *supra* note 41, at 207-227.

A. Some Assumptions of the Institutionalist Approach

The institutionalist approach is a variant of the realist theory of international politics. It thus shares with this theory many assumptions concerning the international system.[43] First, because no higher authority binds individual states, the international system is anarchic. Second, states are the primary actors in the international system, and they act rationally to maximize their power. Third, states functions as "black boxes," in the sense that the internal politics of each state are separable from its activities in the international system.[44] On these assumptions, a state's behavior in the international system can be predicted from the parameters of the system itself and the actions of other states in the system.

The institutionalist view treats international regimes as collective action problems between rational state actors.[45] On this view, international regimes will arise where states must coordinate their behavior in order to achieve a desired outcome. Such a situation might arise where uncoordinated calculations of self-interest will generate a non-Pareto-optimal outcome (such as the classic prisoner's dilemma) or even lead to disastrous results, or where an issue area is particularly complex.[46] The following are typical examples of what institutionalist scholars consider to be regimes: international trade or money regimes (such as the World Trade Organization or the International Monetary Fund), security regimes (such as arms control agreements or the United Nations Security Council), and standardization regimes (such as the International Civil Aviation Organization, the adoption of a common gauge of railroad

---

43. For a more thorough outline of the realist theory of international relations, see HANS J. MORGENTHAU, POLITICS AMONG NATIONS — THE STRUGGLE FOR POWER AND PEACE 3-20 (6th ed. 1985); KENNETH WALTZ, THEORY OF INTERNATIONAL RELATIONS 118 (1979). Morgenthau notes: "The main signpost that helps political realism to find its way through the landscape of international politics is the concept of interest defined in terms of power." MORGENTHAU, *supra*, at 5. *See also* Anne-Marie Slaughter, *The Liberal Agenda for Peace: International Relations Theory and the Future of the United Nations*, *in* PREFERRED FUTURES FOR THE UNITED NATIONS 69-110 (Saul H. Mendlovitz & Burns H. Weston eds., 1995).

44. Stephen D. Krasner gives a more concise version of the realist assumptions: an international system is one of "functionally symmetrical, power-maximizing states acting in an anarchic environment." Krasner, *supra* note 41, at 2.

45. There are interesting parallels between international regime theory and the general theories of social control described by Robert C. Ellickson. *See* ROBERT C. ELLICKSON, ORDER WITHOUT LAW — HOW NEIGHBORS SETTLE DISPUTES 123-240 (1991). To the extent that Professor Ellickson considers law (and hence the state) irrelevant to much of the social order, the order which does arise on his view may resemble that predicted by regime theory for the international system.

46. *See* Krasner, *supra* note 41, at 5-7.

track in Western Europe, or the use of a standard calendar).[47] Thus, while there may be overlap between an international organization and an international regime, the two do not necessarily coincide. This theory has several variants; a full treatment of the differences among them is beyond the scope of this paper.[48] Yet even the broad outlines of the institutionalist approach sketched here suggest that state participation in international regimes can be explained in terms of such considerations as lowering transaction costs and establishing uniform standards of behavior.

B. Institutionalism and the Internet

Characterizing the Internet as an international regime seems eminently plausible. Those states which have permitted Internet access at all have implicitly agreed, at a minimum, to a set of technical standards that facilitate the transmission of data over the Internet.[49] Indeed, it would be almost prohibitively difficult for a single state to declare its non-adherence to the TCP/IP system and remain connected to the Internet. It has been suggested that states connected to the Internet have implicitly agreed to more than mere technical standards. By agreeing to connect to the Internet, the argument goes, the state has acquiesced to a whole set of norms that strictly constrain regulation of the Internet. Yet under our premise that states are capable of regulating cyberspace, and that states act rationally to maximize their own power, there is simply no reason to think that such a broad set of norms will be respected. The power-maximizing state will let the Internet be free only insofar as doing so serves the state's interest. Those norms for which cooperation seems to facilitate the long-term interests of the state will become the governing rule set of the regime, while all others will simply be ignored. To understand which norms might fall into which category, we must examine the structure of the Internet.[50]

Similar to the logic of object-oriented computer programming, the logical structure of the Internet consists of successive levels of abstrac-

---

47. Many of these examples are from Arthur A. Stein, *Coordination and Collaboration: Regimes in an Anarchic World, in* INTERNATIONAL REGIMES, *supra* note 43, at 115.

48. For a broad overview of regime theory see INTERNATIONAL REGIMES, *supra* note 41.

49. The most obvious examples of technical standards are the Internet Protocol (IP) itself, the Transmission Control Protocol (TCP), and the various other low-level standards of the Internet.

50. The rule structure of the Internet is also the subject of extensive treatment in Post, *supra* note 9.

tion, each with a set of standards pertinent only to that level.[51] Thus one level of abstraction on the Internet may interact with other levels without sharing the internal standards of any other level. Consider, for example, the transmission of an e-mail message between hosts in different states. At a low level, agreement on issues such as physical connections, the Internet addressing system, and content-control protocols are necessary for any transfer of data. At an intermediate level of abstraction, agreement on issues such as a standard e-mail protocol and data encryption is important. Finally, at the highest level of abstraction, norms regarding message content become relevant — whether, for example, the message contains forbidden speech. On this model, it seems that the state's interest in imposing its own rules upon Internet processes rises in direct proportion to the level of abstraction. Put simply, the rational power-maximizing state will probably agree with the "functional" (low-level) standards, but impose its own will on "political" (high-level) norms.[52] The abstractions model makes it possible for the state to agree to do just this.[53]

This analysis, however, ignores another set of costs associated with imposing regulation. By hindering the speed and accessibility of the Internet, state control over high-level norms will decrease the economic and other expected benefits of participating in the Internet regime. For example, in Singapore, the coercive use of proxy servers has slowed down Internet access completely, and threatens Singapore's plans to

---

51. This system is formally defined by the International Standard Organization's Open System Interconnect (ISO/OSI) model. The ISO/OSI model recognizes seven layers of abstraction: physical, data link, network, transport, session, presentation, and application. *See ISO/OSI Network Model* (last modified June 28, 1996) <http://www.uwsg.indiana.edu/usail/network/nfs/network_layers.html>. Above these seven layers, which are mostly (but not completely) technical, one can imagine layers corresponding to the human rules and norms that are pertinent to the application in question (e.g., e-mail norms or, more generally, human language).

52. Of course, there are some very real controversies over the functional standards, so to categorize them as totally non-political may be misleading.

53. Interestingly, one branch of international peace theory, known as the "functional approach to peace" and exemplified in the writings of David Mitrany, holds that the encouragement of non-political or functional interactions between states is the best way to build lasting and stable international peace. *See* David Mitrany, *The Functional Approach to World Organization*, *in* THE UNITED NATIONS AND A JUST WORLD ORDER 153 (Richard A. Falk et al. eds., 1991). *But see* Inis L. Claude, Jr., SWORDS INTO PLOWSHARES — THE PROBLEMS AND PROGRESS OF INTERNATIONAL ORGANIZATION 378-407 (4th ed. 1984) (criticizing the functional approach to peace). Mitrany's line of reasoning may be interesting for those who believe the Internet is essentially non-political and may have a role in promoting world peace and unity.

exploit the commercial potential of the Internet.[54] The institutionalist model predicts that power-maximizing states will act to regulate cyberspace as much as possible without threatening the other benefits that the Internet delivers. Let *C* be the control the state exerts over cyberspace, *P* the power it achieves in this way, and *B* the other benefits of Internet participation. In general, *P* will be a positive function of *C*, and *B* will be a negative function of *C*. The state will choose the *C* which maximizes the sum of *P* and *B*. The precise relationship between *P*, *B*, and *C* will shift depending on the technology used for Internet regulation. Where available regulation technology is primitive, the optimal level of Internet regulation will be low. As regulation technology becomes more advanced, however, the optimal level of Internet regulation can be expected to increase. Since technology advances directly with time, this model predicts a future of increasing state regulation of cyberspace. The abstract structure of networks, moreover, can facilitate this regulation by allowing states to pick and choose the norms over which it wants to exercise control without forfeiting participation in the Internet regime as a whole.

There has been some movement to regulate the Internet through international treaty. In the European Union, the Council of Ministers recently endorsed a French proposal for a "Charter for International Cooperation on the Internet."[55] The French Minister for Information Technology expressed hope that the initiative would lead eventually to an accord comparable to the international law of the sea.[56] Such a charter would make the Internet look more like the international regimes familiar to institutionalist theorists.

C. Problems with the Institutionalist Approach as Applied to the Internet

Leaving aside the more general criticisms of the institutionalist approach in international relations theory,[57] we may note at least two reasons to think that institutionalist analysis may fail to yield a satisfying picture of Internet sovereignty. First of all, the institutionalist approach

---

54. *See Not Too Modern, Please: Asia and the Internet*, THE ECONOMIST, Mar. 16, 1996, at 42 (noting the tension between the desire of Asian states to exploit the commercial potential of the Internet and the desire to regulate it). On the definition of proxy servers, see *supra* note 22.

55. For the full text of the resolution endorsing France's proposal, see Council of Ministers Press Release, 1972d Council Meeting, Nov. 28, 1996, *available in* LEXIS, World Library, Txtnws File.

56. *See France Seeks Global Internet Rules*, REUTERS WORLD SERV., Jan. 31, 1996, *available in* LEXIS, News Library, Txtnws file.

57. For a complete criticism, see Slaughter Burley, *supra* note 41, at 225-27.

focuses on the actions of state actors and state regulators. While no discussion of sovereignty can proceed without including state actors, the complete exclusion of individuals and other entities in cyberspace makes the analysis incomplete. It is, after all, not really states that make use of the Internet, but individuals. Few of the international interactions that occur as part of the Internet regime are strictly between states, and it is with such interactions that the realist paradigm is primarily concerned. Second, the realist assumption that states are power-maximizing and homogenous seems inappropriate in the Internet context. Clearly, differing attitudes towards the pre-existing norms of the Internet will lead to widely disparate regimes. The attitudes of "founding" countries like the United States is profoundly different from that of countries for whom the Internet is a somewhat awkward recent arrival.[58] Furthermore, internal considerations such as political processes and preferences may play a large role in determining a state's Internet policy. By examining only external constraints, the realist model ignores these considerations.

The institutionalist analysis of Internet regulation will be most applicable where the behavior of states adheres closely to the realist assumptions of the model. Thus where a state consciously adopts an instrumentalist view of the Internet and deliberately seeks to restrict its use to, for example, what it perceives as economically beneficial purposes, the institutionalist predictions may be accurate. So far, however, there seem to be only a few states that have approached the Internet in this fashion.[59] We now turn to the liberal theory.

IV. THE LIBERAL THEORY OF INTERNATIONAL RELATIONS AND THE INTERNET

A. Assumptions of the Liberal Theory

The liberal theory makes three assumptions about the international system.[60] First, the primary actors in the system are the individuals who constitute domestic societies or groups.[61] Thus liberal theory treats society as analytically prior to the state. Second, governments represent some segment of domestic society.[62] In consequence, state actions are

---

58. For a description of global reactions and attempts to regulate the Internet, see Amy Knoll, *Any Which Way But Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275 (1996).

59. *See supra* notes 30-34 and accompanying text.

60. *See* Andrew Moravcsik, *Taking Preferences Seriously: A Positive Liberal Theory of International Politics*, INT'L ORG., (forthcoming 1997) (manuscript at 4-9, on file with the author).

61. *See id.* at 4-5.

62. *See id.* at 6-7.

seen as a reflection of the interests of that group, expressed through those domestic institutions which link state and society.[63] Finally, and following naturally from the first two assumptions, state behavior will be determined by the configuration and the nature of state preferences.[64] This shifts the emphasis away from state power and external constraints, and towards state purpose and the pattern of demand for international outcomes. Under the liberal theory, these are the essential elements of the international system.

The emphasis on individualized state preferences and heterogeneity leads to significant contrasts between the liberal and institutionalist theories in their predictions concerning relations between like-minded and non-like-minded states.[65] In particular, liberal theory imagines that the kind of cooperation involved in more comprehensive international regimes (like the European Union) depends on states' sharing certain preferences rather than presenting rational solutions to collective action problems.[66] Liberal theory reconceptualizes sovereignty as a much more flexible proposition, especially between like-minded states. This is in stark contrast to a realist "billiard-ball" model of state sovereignty, where state power is sealed in at national borders, and doled out to international regimes only when doing so serves the rational interest of the state.

B. The Shape of Cyberspace Sovereignty under Liberal Theory

Assuming that the states of the world possess effective power to regulate the Internet, to what degree does the liberal theory predict that cyberspace will be left alone? The first observation is that the answer will be different for every state, because states are presumed to be heterogeneous and act according to individualized preferences. Under the liberal model, in some countries cyberspace may be left to govern itself, while in others the government will regulate heavily. Which way the state behaves will depend on whose interests the state apparatus happens to represent. This observation conforms fairly well to the

---

63. *See id.* Various types of governance will give different expressions of society's interests, ranging from tyranny to pure democracy. *See id.*

64. *See id.* at 7-9. In the words of Andrew Moravcsik, "what states do is determined by what they want." *Id.*

65. Evidence often cited to support this proposition includes the apparent tendency of democratic states not to go to war with each other. *See generally* BRUCE RUSSETT, GRASPING THE DEMOCRATIC PEACE: PRINCIPLES FOR A POST-COLD WAR WORLD (1995).

66. *See* Slaughter Burley, *supra* note 41, at 228-30. Professor Slaughter uses the term "sovereignty paradox" to describe this reconceptualization of sovereignty among liberal states that nonetheless maintains a more traditional sovereignty-based view of relations between liberal and non-liberal states at the political level.

observed practice at present, where the degree of regulation varies immensely among nation states.[67]

As under the institutionalist view, it is useful to think of the Internet less as a place and more as a regime of transnational norms and rules (a logical counterpart to transnational law) that regulates international interactions between individuals. These norms and rules may be formally constituted, such as the Internet standards promulgated by the Internet Engineering Task Force,[68] or informal, such as the discourse norms on the Usenet.[69] Such preexisting norms and rules may in themselves generate state behavior that would respect cyberspace sovereignty. Thus cyberspace sovereignty may spring from a consensus among individuals in different states that these rules and norms are reasonable and deserve respect. At the second stage, domestic institutions may transmit this consensus to the state, and a respect for these norms and rules may become a state preference. As Professor Slaughter notes, transnational rules can "structure patterns of individual and group interaction in transnational society, patterns that in turn generate interests that shape and constrain state action."[70] At the third stage, states will modify their behavior in such a way that its actions through code and law include a respect for those norms and rules that it now respects.[71] The result of this process is a minimally sovereign cyberspace, where the

---

67. *See* Knoll, *supra* note 58, at 279-99.

68. For a discussion of the constitution and inner workings of the Internet Engineering Task Force, see generally Paulina Borsook, *How Anarchy Works*, WIRED, Oct. 1995, at 110.

69. For a discussion of informally constituted community norms on the Internet, see generally HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993).

70. Slaughter Burley, *supra* note 41, at 230.

71. This process is familiar in the development of international norms. For example, international human rights norms have tended to spread quickly among the nations that are among the originators, are more slowly to non-like minded states. Interestingly, certain human rights non-governmental organizations ("NGOs") have adopted Internet freedom as a human rights norm, and now press for its respect. The NGOs usually incorporate calls for Internet freedom as part of the right of communication in Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers.*" *Universal Declaration of Human Rights*, G.A. Res. 217, U.N. Doc. A/810, at 71, 74-75 (1948) (emphasis added). For an example of an NGO taking action for the cause of Internet freedom, see Letter from Human Rights Watch Asia to George Yeo, Minister for Information and the Arts, Singapore (August 13, 1996) (protesting Singapore's controls on Internet use). Even members of the U.S. Senate Foreign Relations Committee have protested Singapore's censorship of the Internet. *See* Ray Health, *Lion Closes Net on Rogue Dites*, S. CHINA MORNING POST, Sept. 20, 1996, at 3 (describing the criticism leveled by Senator Russ Feingold at Singapore's censorship of sites critical of its government); *see also* MARK B. FELDMAN, THE RIGHT TO COMMUNICATE UNDER INTERNATIONAL LAW: TOWARDS A LAW OF GLOBAL COMMUNICATIONS 343 (Anne W. Branscomb ed., 1986).

extent of sovereignty corresponds precisely to what the consensus holds to be the proper breadth of freedom from state regulation.

Let us look first at the consensus which serves as the starting point for cyberspace sovereignty under the liberal theory.[72] Individuals, even in the same country, will obviously have disparate views concerning such issues as state interference with freedom of expression. In consequence, their ideas of the appropriate level of Internet regulation will vary. This variation will be even greater among individuals in different states. Therefore, the Internet consensus will be the minimally acceptable set of norms and rules upon which reasonable individual can agree. In practice, the extent of a consensus is likely to be limited in various ways. As noted above, the consensus will likely be broader with respect to "traffic rules," or standards towards the lower end of the abstract structure of the Internet. As for higher-level norms, there are likely to be at least two important constraints. First, where actions in cyberspace have negative secondary effects on real space, a consensus against state regulation of such actions is improbable. For example, most people are likely to agree that control of criminal activity is still the domain of the state. Second, the norms will be more readily accepted by individuals in the United States and similar societies. Because of the pattern of the Internet's growth, most of the currently existing norms have been established by individuals from the United States and like-minded countries; thus the norms of those countries can be felt strongly in the higher-level norms and rules of cyberspace.

In a sense, it is the development of such a consensus that is the true project of the proponents of cyberspace sovereignty. Widespread respect for the Internet regime depends on the reasonableness of the norms and rules proposed, and of the cyberspace institutions that promulgate them. Thus Professors Post and Johnson rightly stress that freedom from state regulation rests on the development of "responsible law making institutions" in cyberspace.[73] What seems untenable, by contrast, is the absolutism of those who claim that state regulation of the Internet is per se unacceptable.[74] While this conception of cyberspace sovereignty

---

72. This notion of overlapping consensus is taken extremely loosely from John Rawls. *See* JOHN RAWLS, POLITICAL LIBERALISM 133-72 (1996).

73. Johnson & Post, *supra* note 5, at 1390.

74. This approach is adopted, for example, by John Barlow. *See supra* note 1. Professors Johnson and Post, to their credit, do advocate a more balanced approach, arguing that the law of sovereigns in the physical world should "defer to this new form of self-government" when cyberspace rules "do[] not fundamentally impinge upon the vital interests of others who do never visit this new space." Johnson & Post, *supra* note 5, at 1394. However, they go too far when they claim that the desire of states to regulate obscenity and its effects is subservient to a "meta-interest" in preserving the free flow of information. *See id.*

certainly has some resonance in the Western world, the foregoing analysis suggests that it is misbegotten with respect to the world at large. For example, appeals to free speech protection of the type guaranteed under the First Amendment will fall on deaf ears in many countries. The proper view, then, is to work toward a level of state regulation about which individuals of widely varying beliefs and world-views can agree. Finally, cyberspace institutions must concede that local governments will have legitimate interests in regulating certain activities and content.

Next, let us consider the transmission of this consensus to the level of state preference. Here, another set of limitations is implicit. Depending on the governing structure, the interests of those who share an international cyberspace consensus may not be adopted as state policy. In a dictatorship, for example, the state's acceptance of Internet sovereignty would depend only on the extent to which the dictator himself believes that the norms and rules of cyberspace deserve respect. Other countries may have other peculiarities in the process of transmitting interests to the government (e.g., powerful lobbies) that affect which interests will determine behavior. Therefore, even in the face of a strong individual consensus that a certain Internet norm deserves recognition by nation states, certain states may nonetheless refuse to adopt the norm.

This leaves us with a generative model of a minimally sovereign cyberspace. It is generative in the sense that it entails a process by which the norms and rules of cyberspace may become respected by a significant number of states. It is minimal in the sense that the only rules and norms likely to gain the acceptance of most states will be those that individuals of widely varying persuasions find acceptable. At this nascent stage of the Internet's influence on mainstream society, cyberspace retains a high degree of independence simply for reasons of inertia. The governments of the world have only begun to express their preferences, and what kind of cyberspace sovereignty will be respected remains to be seen.

V. CONCLUSION

States, their governments, and their citizens ought never be taken for granted as players in cyberspace. It is easy, given the current state of the Internet, to assume that it is and will remain free of external regulation. However, it would be incorrect to adopt such an assumption. A quick empirical look suggests that it is possible to regulate the Internet, and that countries, corporations, organizations, and private individuals are already doing so. This Note has not directly addressed the question of whether regulation of cyberspace by governments is right or wrong. Where states are simply acting to maximize their own power, this question may have little practical relevance. However, as the last Part demonstrates, how individuals feel about this question and whether their interests are

expressed by the state may be crucial in determining the future of cyberspace regulation. The onus, then, is on the developing institutions of cyberspace to develop norms and rules that make sense and will gain broad acceptance internationally.