Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace

Ronald J. Deibert

Millennium - Journal of International Studies 2003 32: 501
DOI: 10.1177/03058298030320030801

Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace

Ronald J. Deibert

Conventional wisdom holds that the Internet's material properties are biased towards openness, and provide the foundation for a global commons of information increasingly beneficial to citizens worldwide. However, pressures from the security and commercial sectors to regulate and control the Internet are beginning to alter its basic material architecture in ways that may undermine not only the activities of global civic networks, but also the long-term prospects for an open global communications environment. As Internet censorship and surveillance becomes more widespread, and as states begin to militarise cyberspace, a radically different environment for global communications is emerging. However, these changes are not uncontested. While not having the influence over Internet security and design issues that security and corporate actors do, a growing number of civil society actors are merging with politically minded computer scientists and engineers to form policy networks and develop 'hacktivist' technologies designed to support self-expression, privacy, and security for global civic networks. For the Internet and other information and communication technologies to support a global commons of information the success of this movement over the long term will be critical.

It has long been a conventional wisdom that the Internet's material properties are biased towards openness, liberalisation, democracy, freedom of speech and communications. Its distributed architecture — a 'network of networks' without central control — has been seen as, among other things, a foundation for a global commons of information, a vehicle for the flourishing of transnational social movements, and a powerful force for democratisation that authoritarian regimes worldwide could not resist. This conventional wisdom has, in turn, not only informed a vast array of state and multilateral initiatives, such as the G8 Dot Force and the UN Information and Communications Task

---

An earlier version of this paper was presented at the International Studies Association Conference, Portland, Ore, February 2003. Thanks to Dorothy Denning, Dan Deudney, Henry Farrell, Bill Mandel, and Rafal Rohozinski for comments on earlier drafts, and Nart Villeneuve for research assistance on the Chinese content filtering data presented here.

Force, but International Relations theorising as well. Underlying most of the many different theories of globalisation and global civil society is an assumption about the 'speed' and 'global reach' of new information and communication technologies, and how these properties have begun to facilitate important changes in the architecture of world order away from a state-based towards a 'network' society.[1]

Whatever the merits of that conventional wisdom, pressures from the security and commercial sectors to regulate and control the Internet are beginning to alter its basic material framework in ways that may undermine not only the activities of global civic networks, but the long-term prospects for an open global communications environment as well. In many ways these pressures to regulate the Internet reflect a natural maturation process that previous media, such as print, radio, and television, all experienced as they evolved out of unrestrained and experimental to tightly controlled and regulated environments. As new information and communication technologies move from the margins to permeate society, economics, and politics, the stakes become much higher and authorities — both public and private — take more of an active interest in how media are designed and secured.[2] Today's Internet is no exception. Whereas once questions of Internet governance were largely determined by technical experts and engineers, today they are increasingly decided by politicians, government officials, lawyers, and military personnel.

These questions of the politics of Internet security and design have taken on a new urgency in the wake of 11 September 2001 and the ensuing global war on terrorism. As will be described below, legislation has been passed in virtually every industrialised country and in many developing countries that expands the capacities of state intelligence and law enforcement agencies to monitor Internet communications. Even more ominous is the very real prospect of an arms race in cyberspace, led by the United States. When combined with the mounting pressures to regulate intellectual property on the Internet coming from the commercial sector, the forces impinging on and shaping the very foundations of global civil society communications are formidable and grow daily.

One intent of this paper is to provide an overview of the current state-of-play with regard to security and design pressures bearing down on the Internet. For those concerned with global democratic communications, mostly this is a rather pessimistic story. If we start from

---

1. The landmark study in this respect is Manuel Castells, *The Rise of the Network Society: Volume I The Information Age: Economy, Society, and Culture* (Oxford: Blackwell Publishing, 1996).
2. See Herb Schiller, *Culture Inc.* (New York: Oxford University Press, 1989).

any ideal perspective on what the communications infrastructure should look like for global civic networks and democracy to flourish (and there is wide variation here to be sure) the current reality offers a fairly bleak picture. As the pressures in favour of military, intelligence, and commercial interests bear down on the Internet, I argue below, the prospects for civic networking and democratic communications become increasingly fragile. The second half of this paper outlines the prospects for contrary forces emerging to censorship, surveillance, and militarisation. Here, the story is not entirely discouraging, as there is a substantial set of social forces combining to bring questions of access, privacy, and diversity to the principles, rules, and technologies that configure global communications. I refer to these social forces as 'civic networks'. Civic networks have begun to create an alternative transnational paradigm of Internet security and design, oriented around shared values and technologies.[3] But their challenges are formidable.

A second, less explicit intent of this paper is more theoretical, and concerns the importance of taking 'material' factors seriously in International Relations theorising. By material factors, I mean not just those traditionally associated with the term, such as military capabilities and modes of production, but the very technologies through which we communicate as human beings as well. Elsewhere — drawing from a long line of theorising in the so-called 'medium theory' or 'media ecology' tradition — I have argued that the media through which we communicate are not 'neutral' or 'empty' vessels, but present specific constraints and opportunities for the nature and type of communications that can take place through them.[4] The 'biases' of communication technologies, as Harold Innis referred to them, shape and constrain the environment within which communications take place.[5] Whatever their many differences, for those who study global democratic governance from a broadly constructivist, discursive and/or critical perspective, and in particular those who are normatively inclined

---

3. For research on the 'social construction of security', see Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998) and Peter Katzenstein (ed.) *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996). I analyse in some depth different 'paradigms' of Internet security in Ronald J. Deibert, 'Circuits of Power: Security in the Internet Environment', in *Information Technologies and Global Politics: the Changing Scope of Power and Governance*, eds. J.P. Singh and James N. Rosenau (Albany, NY: SUNY Press, 2002), 115-42.

4. Ronald J. Deibert, *Parchment, Printing, and Hypermedia: Communication in World Order Transformation* (New York: Columbia University Press, 1997).

5. Harold A. Innis, *The Bias of Communication* (Toronto: University of Toronto Press, 1952).

towards supporting spaces for alternative voices, grassroots democracy, and civil society in its many different variations to flourish, the material properties of the communications environment have at best been taken for granted, and at worst been largely ignored.[6] As the Internet changes, so too do the many consequences that have formed the basis for assumptions made about new communication technologies, including the flourishing of civic networks. Those interested in global democratic governance need to think seriously about the security and design of the communications infrastructure as a constitutive force and material reality, how those properties should be designed in ways that promote, rather than detract from, principles deemed important. At the very least, the communications environment cannot be taken for granted.

The Changing Architecture of the Internet

There was once a time, not that long ago, when serious claims could be made that the Internet was a lawless frontier immune to regulation and control by governments. Libertarian by nature, open in its architecture, the Internet was seen by many as encouraging democracy, freedom, and liberty around the world. Attempts by oppressive regimes to block information were futile.[7] Thanks to this unstoppable, open, liberal architecture, citizens would be able to communicate and deliberate with each other, forming the basis for a single, vibrant global village polity.[8]

---

6. This includes the major works on cosmopolitan democracy, world citizenship, and global civil society, such as Danielle Archibugi and David Held (eds.), *Cosmopolitan Democracy: An Agenda for a New World Order* (Cambridge: Polity Press, 1995); Chris Brown, 'Cosmopolitanism, World Citizenship and Global Civil Society', in *Critical Review of International Social and Political Philosophy* 3, no. 1 (Summer 2001); and Richard Falk, *On Humane Governance* (University Park, PA: University of Pennsylvania Press, 1999); none of whom do more than mention in passing ICTs, let alone consider questions concerning their constitutive nature. An important early work on global civil society, Ronnie D. Lipschutz, 'Reconstructing World Politics: The Emergence of Global Civil Society', in *Millennium: Journal of International Studies* 21, no. 1 (1992), went so far as to dismiss the importance of communication technologies to global civil society — a point I have always considered not only patently absurd in the face of widespread practices to the contrary but counter-productive as well. Ignoring communication technologies leaves them open to colonisation by security and commercial sectors, as outlined below. For more on these points, see footnote 72 .

7. See, for example, Michael A. Froomkin, 'The Internet as Source of Regulatory Arbitrage', in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure,* eds. Brian Kahin and Charles Nesson (Cambridge, MA: MIT Press, 1997), 129-63.

8. For representative views, see John Perry Barlow, *A Declaration of the Independence of Cyberspace,* (February 1996) http://www.eff.org/~barlow/Declaration-Final.html; and George Gilder, Telecosm, (New York: Free Press, 2000).

To be sure, there is a great deal of evidence to support this conventional wisdom. Researchers have established a strong correlation between ICT connectivity and democracy and openness worldwide. In one of the more well known of these studies, Christopher Kedzie argued that '[t]he recent innovations in new communication media markedly stand out from previous technologies in fundamental ways that tend to bias political outcomes in favor of greater societal openness and freedoms.'[9] Kedzie and others argued that ICTs played a major role in the transformations that brought an end to former communist regimes in the Soviet Union and Eastern Europe. These regimes were unable to develop a post-industrial society without also losing grip over their population's democratic aspirations.[10]

As researchers have investigated how the Internet emerged and how it has been governed over the course of its evolution, this conventional wisdom has been increasingly called into question. Standing out as a landmark in this respect has been the work of the legal scholar Lawrence Lessig.[11] Although his central theoretical point — that code is not neutral or transparent but actively shapes what can be communicated and how — would not be considered novel by media ecologists,[12] it demonstrated convincingly to a wide audience that the architecture of the Internet should not be taken for granted. From this perspective, many of those prior conventional wisdoms about the open, liberal character of the Internet and its many attendant consequences reflect less some inherent 'nature' than they do the properties of the technology at a specific moment in time. Media certainly facilitate, shape, and constrain the possibilities of human communication, but it is important to keep in mind that media themselves evolve over time as well. We are living through such a time today. Across several interrelated dimensions, it appears that Internet's 'lawless frontier' is quickly closing. Taken individually, these changes eat away at some of the important foundations that would have to be incorporated into any

---

9. Christopher R. Kedzie, *Communication and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma* (RAND, RGSD-127, 1997).

10. See also Audrey N. Selian, 'ICTs in Support of Human Rights, Democracy, and Good Governance', *International Telecommunications Union* (August 2002).

11. See in particular Lawrence Lessig, *Codes and Other Laws of Cyberspace* (New York: Basic Books, 2000).

12. See, for example, Deibert, *Parchment, Printing, and Hypermedia: Communications in World Order Transformation* (New York: Columbia University Press, 1997); Harold A. Innis, *Empire and Communication* (Oxford: Oxford University Press, 1952); and Marshall McLuhan, *Understanding Media* (New York: McGraw Hill, 1964).

communications infrastructure for global democratic governance, such as diversity, access, openness, and privacy. When combined, they present a rather bleak future indeed.

Censorship

Censorship is defined as the act or system of practice suppressing, limiting, or deleting objectionable or any other kind of speech. Although all political regimes engage in some forms of censorship, liberal democratic polities have distinguished themselves from illiberal polities on the basis of limitations on censorship and accompanying protections of free speech.[13] Freedom of speech is constitutionally enshrined in many liberal democratic states around the world, and it is one of the cornerstones of the United Nations Declaration of Human Rights (Article 19). As alluded to earlier, the Internet has long been seen as providing a technological fortification for free speech. It has been a remarkable forum where citizens can publish their views to a worldwide audience, communicate in an unrestricted fashion with other citizens, and in doing so create new communities of interest. Social forces are emerging, however, that have begun to chip away at that technological fortification. The most direct assault comes from increasingly sophisticated forms of state content filtering, described below. A more unlikely source comes from intensifying pressures to regulate intellectual property and copyright, to which we now turn.

Commercial Censorship

As information has become increasingly digitised, so have a wide range of consumer products, including movies, music, and books. Although entertainment, software, and other commercial industries have sought to capitalise on new means of distributing their products through digital networks, they have had to face the problem of the theft of intellectual property and copyright violations.[14] Once digitised and placed on distributed networks, information is easy to duplicate and distribute. Companies and their lobbyists in the affected industries, such as the Recording Industry Association of America (RIAA) and the Motion

---

13. John Stuart Mill, *On Liberty*, Chapter One: 'This, then, is the appropriate region of human liberty. It comprises, first, the inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological'.

14. The question of 'securing' ideas, which forms the basis of contemporary intellectual property issues, is a topic I deal with in some detail in my forthcoming *The Politics of Internet Security: Guarding the Global Commons* (forthcoming: MIT Press).

Picture Association of America (MPAA), have claimed large losses in potential sales, though determining figures with precision rests on questionable counterfactuals. To take one example, losses to the worldwide software industry caused by the use of unlicensed software were said to amount to US$10.97 billion in 2001, according to a report by the anti-piracy organisation Business Software Alliance (BSA).[15]

Not surprisingly, these powerful social forces of the new economy have taken or supported increasingly strident measures to protect their property and preserve copyright in cyberspace. To be sure, there are good reasons to support intellectual property and copyright as a source of innovation, creativity and indeed freedom of speech itself. Without a system of incentives to ensure appropriate recompense for expended resources, and protections against theft and plagiarism, the circulation of ideas essential to a liberal democratic society could wither. However, the application of long-standing principles of intellectual property and copyright to 'knowledge' and 'information' has proven difficult in practice, leading to subtle (and not so subtle) restrictions of creativity and self-expression.[16] Approaches range from the introduction of new laws at both the domestic and international levels, new forms of industry practice, and, perhaps most consequentially, the development of new codes built directly into the communication media themselves.

One of the more notorious measures is the Digital Millennium Copyright Act (DMCA), an act of US Congress that was signed into law on 28 October 28 1998 by President Clinton, and whose purpose is to update US copyright laws for the digital age.[17] According to a study by the Electronic Frontier Foundation on the Unintended Consequences of the DMCA, the DMCA has been employed as a tool of anti-competition, has stifled legitimate research into cyber-security and encryption technologies, and has undermined 'fair use'.[18] To give just a few egregious examples, a garage door opener company has employed the DMCA to prevent rival companies from developing universal remote

---

15. See the *Seventh Annual BSA Global Software Piracy Study* (June 2002) http://www.bsa.org/usa/policyres/admin/2002-06-10.130.pdf.

16. For accessible discussions, see Siva Vaidhyanathan, *Copyrights and Copywrongs: The Rise of Intellectual Property and How it Threatens Creativity* (New York: New York University Press, 2001); and Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Random House, 2001).

17. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf.

18 Electronic Frontier Foundation, Unintended Consequences: Three Years Under the DMCA (3 May 2002) http://www.eff.org/IP/DMCA/20020503_dmca_consequences.pdf.

controls that operate on its system.[19] Computer scientists working on encryption systems have been scared away from their research by legal threats from industry groups who claim proprietary ownership over the codes employed to prevent piracy.[20] The DMCA and other laws have also impinged on academic databases and the circulation of electronic journals, once one of the unmistakably positive elements of the Internet. Many believe the restrictions are leading to the suffocation of works in the public domain for scholarship and a wholesale erosion of the global commons of information.[21]

The DMCA may seem heavy handed, but it pales in comparison to some of the more aggressive pieces of legislation that have yet to pass the bar and provide a general indication of legal trends. United States Representative Howard Berman introduced legislation in 2002, called the P2P Privacy Prevention Act[22] that would grant copyright holders near-immunity from the law while using hacking attacks against computers that are suspected of trading illegally copyrighted material over peer-to-peer (P2P) networks — a startling legitimisation of cyber-vigilantism. Other legal measures have targeted Internet Service Providers (ISPs), holding them accountable for traffic that flows through their networks and requiring them to turn over user information.[23] By imposing the responsibility to monitor traffic to the ISP level, such legislation blurs long-standing distinctions between 'content' and 'carriers' considered vital to free speech. More practically, it would raise costs prohibitively, forcing smaller service providers out of the market, thus limiting access and facilitating monopolies through vertical integration.

While most of these measures are centred in the United States, they have become increasingly internationalised through similar legislation being adopted in other countries. The United States Trade

---

19. For references, see 'DMCA vs. Garage Door Opener', at Politech, http://www.politechbot.com/p-04319.html.

20. Jonathan Band, 'Congress Unknowingly Undermines Cyber-Security', *SiliconValley.Com* (16 December 2002) http://www.siliconvalley.com/mld/siliconvalley/4750224.htm?template=contentModules/printstory.jsp.

21. For discussion, see J.H. Reichman and Paul F. Uhlir, 'Promoting Public Good Uses of Scientific Data: A Contractually Reconstructed Commons for Science and Innovation'. Paper produced as part of the Conference on the Public Domain, Duke Law School, 9-11 November 2001. This paper and others from the conference can be found online at: http://www.law.duke.edu/pd/papers.html#history.

22. See http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.05211.

23. See Michelle Delio, 'RIAA's Rosen Sets Sights on ISPs', *Wired* (22 January 2003) http://www.wired.com/news/print/0,1294,57326,00.html

Representative has pushed the DMCA in bilateral trade negotiations,[24] and many of its main elements are manifest in treaties administered by the World Intellectual Property Organization (WIPO). Among other things, the internationalisation of the DMCA has raised questions about the relationship between intellectual property and development. Although there is good evidence that the introduction of strong intellectual property laws encourages foreign direct investment, some have begun to explore ways in which intellectual property laws create new forms of dependency, locking businesses into monopolistic chains of exchange and preventing local entrepreneurship.[25]

Some of the limitations on free speech have emerged not through regulation but through changes in industry practices, such as new forms of broadband access. Although the latter would seem prima facie to support self-expression and civic communications by expanding the volume of traffic available to users, broadband access, particularly cable, can create serious limitations on free speech.[26] Unlike dial-up access to the Internet, which falls under open 'common carriage' regulations central to the telecommunications industry, cable access is bound by no such restrictions on controlling content and is subject to far greater centralised control. Common carriage policies require that network owners do not discriminate against information by halting, slowing, or otherwise tampering with traffic that flows through them. Cable providers, on the other hand, are under no obligation to remain a neutral pipe for content over end-to-end communications. Cable Internet access providers can and often do control the overall speed of customers' connections, limit access to specific approved technologies and applications such as Internet telephony and virtual private networks, 'push' favoured content and applications, monitor email and websurfing patterns, and tamper with connections to certain types of Internet content, including sites not falling within the cable companies' 'family of businesses. As a recent American Civil Liberties Union (ACLU) report noted, the latter is 'like a phone company being allowed to own restaurants and then provide good service and clear signals to

---

24. For one example, see Simon Hayes, 'US Tightens Net Copyright', *News.Com.Au*, (28 January 2003) http://www.news.com.au/common/printpage/0,6093,5896759,00.html.

25. See K. Aoiki, 'Neocolonialism, anticommons property, and biopiracy in the (not-so-brave) new world order of international intellectual property protection', *Indiana Journal of Global Legal Studies*, 6, no.1 (1998).

26. See *No Competition: How Monopoly Control of the Broadband Internet Threatens Free Speech*, (ACLU White Paper) http://archive.aclu.org/ issues/cyber/NoCompetition.pdf.

customers who call Domino's and frequent busy signals, disconnects, and static for those calling Pizza Hut.'[27] When viewed in light of ever-increasing forms of industry consolidation, which in turn restricts freedom of choice, these forms of content control appear even more ominous.

Perhaps of most concern are measures taken to protect intellectual property and copyright through technical means; in particular through the introduction of codes built into the software and hardware that structure permissible communications.[28] Microsoft's Palladium[29] and Intel's Trusted Computing Software Alliance build into their products code to enforce digital rights management, so that software communicates securely with vendors. Once installed, the codes prevent applications other than those that fall within the trusted platform as a whole from working, building into the architecture a kind of soft vertical integration. Apart from the restriction of choice and user innovation, such initiatives could create a new dependency around major vendors like Microsoft, especially for the developing world.[30] More broadly, such initiatives foment a litigious environment around electronic communications that in turn could lead to self-censorship. You know something does not square properly for the notion of the public sphere when explicit consent must be given to lengthy legal documents before installing a piece of software, viewing a downloaded movie, or entering a chat room — now a commonplace part of the cyberspace experience.[31]

While directed at the illegal trading of software, music, and video files, legislation and activities such as those outlined above are having the unintended effect of overriding technologies and communicative practices that are used and should be considered vital to support civic networks, such as open source software, P2P network systems, and a global commons of information in the open public domain. What makes these new laws so draconian, as Lawrence Lessig in particular has argued, is that their enforcement can now be implemented by code — in

---

27. Ibid.

28. An extended discussion can be found in Lessig, *Code*.

29. Under pressure from those who oppose the technology, Microsoft has renamed Palladium, 'next generation secure computing base'.

30. See Hal R. Varian, 'New Chips Can Keep a Tight Rein on Consumers', *New York Times* (4 July 2002).

31. Illustrating the extent to which such legal consents embodied in code can go, Network Associates, a maker of popular antivirus and computer security software, attempted unsuccessfully to require users to get permission from the company before writing reviews of its products. See Matt Richtel, 'Court Rules Against Network Associates' Software Review Policy', *New York Times* (18 January 2003). The New York Supreme Court struck down the policy as unconstitutional.

other words written into the very architecture of the Internet itself.[32] Such a shift in intellectual property regimes would not just affect a compartmentalised sphere of activity on the Internet or ensure that piracy is stemmed (although even that is debatable in a digital environment). Rather, it would affect the very architecture of the Internet, corralling online communications into channels that support information consumption and the so-called knowledge economy, while stifling the democratic exchange of ideas essential to any model of global democratic governance.[33]

State Censorship

One of the conventional wisdoms about the Internet outlined earlier is that states cannot control Internet communications.[34] State attempts to impose censorship on content in the 1990s were regularly and quickly outflanked by the Internet community, as free speech advocates and cyber-libertarians quickly posted mirror sites of the banned content. Not surprisingly, many observers extrapolated far-reaching implications for state sovereignty tied to the properties of digital electronic communications.[35] While global flows of communication have made state censorship difficult, to be sure, they have not made it impossible. Many states around the world, assisted by new censorship technologies, have put in place highly developed Internet content filtering systems that place national controls on what type of information their citizens can access over the Internet.[36] When accompanied by contextual factors, such as severe regulations and stiff penalties imposed on user activities and ISPs, these tools have begun to carve out national censorship islands within the global flow of information.[37]

---

32. Lessig, *Code*.

33. For a critique of global civil society from the perspective of communications and consumption, see Edward Comor, 'The Role of Communication in Global Civil Society: Forces, Processes, Prospects', *International Studies Quarterly* 45 no. 3 (September 2001).

34. See Froomkin, 'The Internet as a Source of Regulatory Arbitrage'.

35. See, for example, Walter Wriston, *The Twilight of Sovereignty* (New York: Scribner, 1992).

36. For a detailed but somewhat dated technical overview, see Philip McCrea, Bob Smart, and Mark Andrews, *Blocking Content on the Internet: A Technical Perspective.* A Report Prepared for the National Office for the Information Economy, (June 1998) http://www.cmis.csiro.au/projects+sectors/blocking.pdf.

37. For overviews, see Human Rights Watch, *Freedom of Expression on the Internet*, Annual Report 2000 http://www.hrw.org/wr2k/Issues-04.htm; and Reporters Without Borders, Enemies of the Internet http://www.rsf.org/ennemis.php3. See also Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (New York: Carnegie Endowment for International Peace, 2003).

One of the problems determining the extent of Internet censorship is the lack of information, as states have withheld such information for security purposes. In recent years, several human rights organisations have issued lengthy descriptions of Internet and other media censorship, some of which have evolved into regular annual reports.[38] Press reports and other accounts have begun to build a general picture of censorship across a broad range of countries, from European countries like Germany to developing countries like China. While empirical knowledge of Internet censorship is still very much in its infancy, studies undertaken by the author in collaboration with researchers at the University of Toronto, Harvard University and University of Cambridge have begun to employ network interrogation tools that excavate the Internet directly for evidence of content filtering.[39]

The Internet censorship regime in China is broadly composed of a combination of: self-censorship; legal restraint and fear of punishment; content filtering software (usually implemented in Internet Cafés); and a national firewall at the Internet backbone level designed to block access to Internet content deemed 'undesirable' or 'subversive'.[40] Although it is known that China employs content filtering, little is known about what or how much, precisely is being blocked — a state secret. A study undertaken under the direction of the author analysed Internet blocking at China's national backbone level. There are nine backbone networks according to the China Internet Network Information Center and there are differences in blocked content among the networks. Using technical means to connect to proxy servers on three national backbones, the author's research team tested 8878 URLs in a number of different categories, such as religion, human rights, and minorities. The results indicated not only that upwards of 20 per cent of the tested URLs were blocked across categories ranging from ethnic minorities to the banned religious group Falun Gong, but that the technology enabling the blocking was provided by a Western corporation, Cisco Systems Inc.[41]

Some of the more aggressive content filtering systems have been adopted in Arabic and Islamic regimes. While these countries admittedly block access to pornographic sites, they have also begun to

---

38. See footnote 27 above.

39. The following research draws on previously noted studies and reports, as well as primary research undertaken as part of the Open Net Initiative project, a collaboration of the Citizen Lab, University of Toronto, the Berkman Centre for Internet & Society, Harvard Law School, and the University of Cambridge, UK. See http://opennetinitiative.net/ for detailed overviews and reports.

40. For extended discussion, see Ronald J. Deibert, 'Dark Guests and Great Firewalls: Chinese Internet Security Policy', *Journal of Social Issues* 58, no. 1 (2001): 143-58.

41. See http://opennetinitiative.net/ for the original Project C report.

employ the same filtering technologies to block political websites, particularly human rights websites critical of their regimes' records.

Saudi Arabia, for example, has had Internet connections since 1994, but these were restricted to special segments of the population until 1997, when Saudi citizens were allowed to use modems to dial-in through expensive international connections. It was not until 1999 that the Internet was opened up to the wider general public — a delay due to the interest of the authorities in establishing a content filtering system. Internet regulations are laid out in the Saudi Council of Ministers Decision Number 163, made public in May 1998, which requires ISPs and users to refrain from 'using the network for illegitimate purposes such as, for example, pornography and gambling; ...carrying out any activities violating the social, cultural, political, media, economic, and religious values of the Kingdom of Saudi Arabia; sending or receiving coded information unless after obtaining the necessary licenses from the administration of the network in question; [and] introducing others into the usage accounts or briefing them on the secret number of the user.'[42] Using a Western corporate technology called 'Websense', the Saudi regime blocks not only pornographic and political websites, but specific pages within websites as well. Some human rights websites, for example, are accessible to Saudi Internet users, but not pages related solely to the Saudi regime. Similar systems of censorship and control exist in Bahrain, Jordan, Syria, Tunisia, Pakistan, the United Arab Emirates, and Yemen, among others.

Many other developing countries have also modelled their Internet regulatory environment on these states' content filtering regimes, using the excuse of the war on terror to build Internet censorship and surveillance strategies. Observers of East Asia have documented a tightening grip over the media recently, including the Internet. Independent media in Indonesia and Malaysia that benefited from liberalisation beginning in the late 1990s, for example, have faced heavy crackdowns, censorship, and state surveillance in recent years. In November 2001 the Indonesian Parliament established a national broadcasting commission with the power to revoke licences or censor content, and stopped TV and radio stations from re-broadcasting foreign programs. Police in Malaysia forced the temporary closure of website Malaysiakini.com in January 2003 after it published a letter questioning the special economic rights accorded to native Malays.[43] Although our research has only established some initial findings in countries other

---

42. See Human Rights Watch, *Freedom of Expression on the Internet*, Annual Report 2000 http://www.hrw.org/wr2k/Issues-04.htm.

43. See Alan Boyd, 'Dark Days for Asian Journalism', *Japan Today* (1 February 2003) http://www.japantoday.com/e/?content=comment&id=330.

than China, using technical means we have so far determined that Internet filtering technologies have been used in Singapore, Vietnam, and Myanmar (Burma) to block political sites.[44]

The picture that emerges from both surface press accounts and more extensive empirical research shows an Internet that is much more of a patchwork quilt than a borderless world of free-flowing information.[45] Such censorship strategies, employed in many cases with Western technologies, restricts the capacity of civic networks to disseminate information both at home and abroad, harming information and education initiatives along with lobbying efforts and awareness campaigns. Furthermore, it constrains the researching, networking and resource sharing opportunities of NGOs and civic networks with other domestic and international NGOs by effectively blocking email access, websites and other Internet services.

Electronic Surveillance

An important lever of modern state power has always been the ability to eavesdrop on and collect electronic information. During the Cold War, massive resources were directed to electronic espionage, including the creation of an international network of signals intelligence that included the United States, Canada, the United Kingdom, Australia and New Zealand.[46] In liberal democratic states, regulations were enacted over time that restricted the type of information that could be collected and what could be done with it once collected; although some areas, particularly intelligence, operated with little oversight and control. At the least, most liberal democratic states maintained sharp divisions between domestic law enforcement and foreign surveillance and information collection as way to check and constrain the centralisation of power.

After 9/11, however, legislation has been quickly adopted by many states around the world that paves the way for a far more permissive environment for electronic surveillance and the sharing of information among domestic law enforcement and foreign intelligence. Specific state legislation along these lines includes Canada's Bill C-36 and Bill C-17,

---

44. See the Open Net Initiative Project at http://opennetinitiative.net/ for expanded details on our research in this area.

45. This is also the conclusion of Kalthil and Boas, *Open Networks, Closed Regimes.*

46. James Bamford, *Body of Secrets: Anatomy of the Ultra Secret National Security Agency* (New York: Anchor Books, 2002); Matthew M. Aid and Cees Weibes, *Secrets of Signals Intelligence During the Cold War and Beyond* (London: Frank Cass, 2001).

the United States Patriot Act, and the United Kingdom Crime and Security Act. At the international level, the Council of Europe's Cybercrime Treaty, while initiated prior to 9/11, has been beefed up significantly since. The Cybercrime Treaty has become a major legislative node that includes not only European powers, but potentially states outside Europe as well, such as Canada, Australia, South Africa, and the United States; all of whom will have to make domestic adjustments to its invasive provisions once ratified. Among other controversial elements, the Treaty allows for intrusive wiretaps that allow for the real-time collection of traffic, forces individuals with knowledge of security methods related to data of concern to reveal them under force of law, and places extraordinary responsibilities on ISPs to collect and archive content for 'lawful access'.[47] Although each of these pieces of legislation differs, what they have in common is the introduction of a substantially more permissive environment for the use of electronic wiretaps, the collection of email and websurfing data, and the sharing of information between law enforcement and intelligence agencies, both domestically and internationally.[48]

Electronic surveillance has been augmented not only by new regulations but by new technologies, including video surveillance systems, biometric and facial recognition technologies, and 'smart' identification cards. Both Australia and Canada, for example, have introduced controversial plans to keep security databases on travellers leaving and entering the country. Many of these new technologies have been introduced without accompanying regulations on usage. In the area of video surveillance, for example, many countries have no limits on what can be done with the data once collected. In some countries, like the United Kingdom, the data derived from public and private video surveillance technologies is already being actively integrated into intelligence collection operations.[49]

---

47. Although not an international treaty per se, the US Communications Assistance for Law Enforcement Act (CALEA) requires telephone common carriers to design their systems to allow for the isolation and routing of calls so that they can be intercepted by law enforcement. As most major international carriers are of US origin, the CALEA essentially internationalises US surveillance regulations in practice.

48. Such regulations have not been limited to the Northern industrialised countries. In the immediate aftermath of 9/11, for example, several Central Asian countries rapidly reassessed their policies with regard to the development of the Internet, preferring to frame them within the context of national security as well as national development. Other developing countries have followed suit.

49. Mark Townsend and Paul Harris, 'Security Role for Traffic Cameras', *The Observer* (9 February 2003) http://www.observer.co.uk/politics/story/0,6903,892001,00.html.

The surveillance system that generated the most alarm among privacy advocates was the Pentagon's Total Information Awareness Office (TIAO), led by the notorious John Poindexter of Iran-Contra fame. Although the details of this new office were fuzzy, early reports indicated that it would aim to create target profiles of suspicious activities by culling through integrated databases drawing from all electronic communications, such as consumer financial transactions, email, and websurfing.[50] The controversial office alarmed many privacy advocates and quickly became the object of concerted outrage and web activism. In what only seemed to fuel the flames of concern, the TIAO responded by gradually eliminating details from its website. At the time of writing, the US Congress has frozen the budget for the TIAO, and there are plans to revise it with some limited oversight.[51] However, the office's ambitious plans for total electronic surveillance illustrate the radically changing security environment within which Internet communications now take place.

So far, the surveillance outlined has been limited to that which takes place on behalf of law enforcement and intelligence. For decades, commercial organisations have been undertaking analogous surveillance practices targeting consumer purchasing and transaction habits both on and offline.[52] From the use of 'cookies' to track websurfing to the collation of credit card purchases to the use of Closed Circuit Television (CCTV) cameras in private and public space, corporations have gathered a wealth of information on individuals' habits from new ICTs. What makes them more troublesome today, however, is the prospect not only of the relaxation of privacy laws designed to restrain such practices, but the increased porosity of commercial and state databases due to post- 9/11 security legislation.

Given all of these new surveillance measures and tools, privacy advocates and civil society networks around the world have not surprisingly reacted with extreme distress. Noting the changing regulatory environment post 9/11, the NGO Reporters Without Borders said that the Internet had become part of the 'collateral damage' of the war on terror.[53] A report by the American Civil Liberties Union noted with alarm that the new surveillance regimes being imposed in the

---

50. See Lauren Weinstein, 'Year In Privacy: Citizens Lose', *Wired* (30 December 2002) http://wired.com/news/privacy/0,1848,56954,00.html.

51. Adam Clymer, 'House, Senate Agree to Prohibit Citizen's Email Surveillance', *New York Times* (12 February 12 2003).

52. See David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis, MA: University of Minnesota Press, 1994).

53. Reporters Without Borders, *The Internet on Probation* http://www.rsf.fr/article.php3?id_article=3671.

United States 'will place millions of innocent Americans under government scrutiny in an epidemic of privacy invasions'.[54] In spite of these and many other pleas, the shocks of 9/11 have seemingly precipitated a wave of new electronic surveillance measures. These measures fundamentally alter the environment within which Internet communications take place. NGOs and civil society networks, particularly in human rights and humanitarian areas and those working in repressive regimes, are of course most immediately affected. But the intensification of surveillance practices raises much deeper concerns about the nature of electronic communications for global democratic governance. Much like freedom of speech, liberal democratic societies depend on and value strong protections for privacy. While at one time the Internet may have enabled privacy through anonymous communications, all signals today point to its rapid dissolution.

Militarisation of Cyberspace

Accompanying electronic surveillance has been the largely undebated militarisation of cyberspace. A great deal of attention has focused on the question of cyberterrorism, particularly in the wake of 9/11 and fears of potential terrorist use of electronic networks.[55] While some see the possibility of an 'electronic Pearl Harbour' being unleashed by terrorists, skilled individuals and non-state actors, many others believe these fears are largely overdrawn and ignore the redundancies built into the architecture of the Internet as well as the relatively low pay-off for groups whose ultimate aim is violence.[56] In spite of the alarm, there are no empirical examples of cyber-terrorism to date, unless the term is used so broadly as to encompass politically motivated hacks on websites and occasional inconveniences caused by denial of service attacks. Rather than tools of mass destruction, threats from terrorist actors employing the Internet appear to bode little more than periodic disruptions to Internet traffic.[57]

---

54. Audrey Hudson, 'Supersnoop Scheme Pending Review', *Washington Times* (13 February 2003).

55. See, for example, Dorothy Denning, 'Is Cyber Terror Next', in *Understanding September 11th* ed. Craig Calhoun (New York: New Press, 2002).

56. For an extended analysis that takes this position, see James A. Lewis, 'Assessing the Risks of Cyber Terrorism', *Center for Strategic and International Studies* (December 2002).

57. Steve Alexander, 'Some Experts Say Cyberterrorism is Very Unlikely', *Star Tribune* (13 February 2003) http://www.startribune.com/stories/535/3650296.html.

Whatever the ultimate nature of the threat, the debate has largely obscured a potentially more serious development: the quiet expansion and adoption of offensive information warfare capabilities by states. The military use of cyberspace operates on a new terrain, presenting many thorny legal and moral questions concerning the targeting of civilian infrastructures, and the boundaries between an armed assault, a probe, the collection of information, and the dissemination of propaganda.[58] Theory has definitely trailed behind practice in this case.[59]

As in most areas of military capabilities, the United States leads the cyber arms race. The development of cyber-war tools can be seen as a natural evolution of the so-called Revolution in Military Affairs (RMA), the latter defined as a major change in the nature of warfare brought about by the innovative use of new technologies and organisational structures related to them; from advanced computing and communications technologies to remote sensors.[60] Going back further, its roots can be found in the use of propaganda and psychological warfare techniques and electronic jamming that date to the Second World War: electromagnetic pulse bombs (EMPs), and the insertion of malicious codes and secret back doors in software for intelligence purposes during the Cold War. While much of these techniques were kept clandestine, the United States has recently acknowledged that offensive cyber-war is an official element of strategic doctrine.[61] The United States' military now openly employs computer hackers, develops advanced Trojan horses, viruses, and worms, and has used techniques of cyber-propaganda and other sophisticated 'psychological operations' leading up the conflict in Iraq.[62]

It is not alone. Dozens of countries around the world have either debated or adopted offensive cyber-war capabilities, including China, Russia, Taiwan, Israel, the United Kingdom, Australia, and Canada. The number of documented state cyber-war has risen in recent years as well.

---

58. See Lawrence T. Greenberg, et al., *Information Warfare and International Law* (Washington DC: National Defense University Press, 1998).

59. The one exception has been the work of James Der Derian. For an early and still very insightful work, see James Der Derian. 'The (S)pace of International Relations: Simulation, Surveillance, and Speed', *International Studies Quarterly* 34 (1990): 295-310.

60. For a general discussion, see Zalmay Khalilzad, John P. White, and Andrew W. Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare* (Santa Monica, CA: RAND, 1999).

61. Bradley Graham, 'Bush Orders Guidelines for Cyber-Warfare', *Washington Post* (7 February 2003).

62. See Dan Caterinicchia, 'DOD Plans Network Attack Task Force', *Federal Computer Week* (7 February 2003) http://www.fcw.com/fcw/articles/2003/0203/web-net-02-07-03.asp.

In spite of the greater penetration of these technologies in advanced industrialised countries, many of the more prominent examples of information warfare have occurred in the developing world.[63] It is, of course, well known that radio networks were employed by Tutsi militia to incite genocidal violence against Hutus in Rwanda. Later, the Rwandan military regularly eavesdropped on insecure United Nations and humanitarian NGOs' communications networks, and in at least one case used the intelligence to hunt down and kill Hutu refugees.[64] During the Russian campaign against Chechnya in the mid-1990s, Chechen commanders made efficient use of mobile phone networks and eavesdropped on insecure Russian radio networks to organise devastatingly successful military strikes. In 2000, an 'inter-fada' erupted between Israeli and Lebanese hackers as each bombarded the other's networks in distributed denial of service attacks. In the 2002 re-occupation of Palestine by the Israeli Defence Forces (IDF), the IDF systematically targeted the communications and information infrastructure of the Palestinian Authority and other civil society groups in tactics ranging from removing hard drives to disabling telephone switchboards.[65]

What are the concerns for global civic networks of the militarisation of cyberspace? In some respects, the threats may be exaggerated. Just as networked redundancies and distributed security practices constrain the potential ramifications of cyber-terrorism, there may be natural limits to the type of havoc states can wreak on the global communications infrastructure. There are also rational, as well as technological, constraints. Much like the deterrent effect of nuclear weapons, states that are home to private corporations with assets spread transnationally throughout the world face strong financial incentives to preserve the security and seamless functioning of global communications networks that are the sinews of hyper-capitalism. These constraints should not be overdrawn, however. Rational choice models of costs and benefits do not always translate neatly into the equations drawn for the use of force internationally. And even targeted attacks on infrastructures can cause enormous disruptions to the flows of information worldwide, as several recent worms and viruses have demonstrated.

More broadly for global democratic governance, however, is a theoretical question about the proper constitutive relationship between

---

63. This section draws from Rafal Rohozinski, 'Bullets to Bytes: Reflections on ICTs and "Local" Conflict', in *Bombs, Bytes, and Bandwidth* ed. Robert Latham (New York: New Press, 2003).
64. Ibid.
65. Ibid.

military and civilian spheres in liberal democratic polities; particularly as these bear on questions concerning the design of the public sphere. The Internet is much more than a simple appendage to other sectors of world politics — it is the forum or commons within which civic communications will take place. Preserving this commons from militarisation is as essential to global democratic governance as is the judicial restraint on force in domestic political spheres. Given the race by states to develop offensive information warfare capabilities, and its potentially destructive and unforeseeable consequences, has the time come for a kind of cyberspace 'arms control'? If so, what might that look like and how might it emerge?[66] Though not described in terms of arms control per se, the following section offers a survey of the prospects.

Transnational Information Security and Global Civil Society?

The time has long since passed when it would be beneficial for global democratic governance and civic networks to allow the Internet to evolve on its own. Although its initial open, liberal architecture provided an enormous boost to civic networks around the world, changes outlined above have begun to alter its root characteristics. As it stands to date, these changes overwhelmingly reflect the interests of businesses on the one hand and states' military and intelligence agencies on the other.[67] These social forces have different conceptions of what constitutes a threat, what is to be protected, and what should be the prevailing design of the global communications infrastructure, and they have considerable resources at their disposal to bring those interests to fruition. Unless a transnational social movement arises to bring to bear on Internet governance the concerns of civic networks — an open commons of information, freedom of speech, privacy, and distributed grassroots communications — the prospect of building a communications infrastructure that supports, rather than detracts from, global democratic governance will become increasingly difficult. The remainder of this paper outlines some of the constraints and opportunities of such a social movement emerging,[68] beginning with the two solitudes of civil society actors and information technology specialists.

---

66. For a discussion of 'cyberspace arms control', see Dorothy Denning, 'Obstacles and Options for Cyber Space Arms Control', presented at Arms Control in Cyberspace, Heinrich Böll Foundation, Berlin, 29-30 June 2001 http://www.cs.georgetown.edu/~denning/publications.html.

67. For an extended discussion, see Deibert, 'Circuits of Power', 115-42.

68. Although I hesitate to use the language of 'counter-hegemony' because of its Gramscian connotations, and the class emphases that go along with it, my concentration on contrary social movements and social forces is heavily influenced by the writings of Robert Cox.

Two Solitudes

From local grassroots movements in rural Ontario to NGOs in Zambia, ICTs, including the Internet, are the information infrastructure — the material nerves — of civic networks around the world.[69] ICTs have become more than an incidental appendage. Much as in other spheres of society, economics, and politics, they have insinuated themselves integrally into all of the different facets of what these groups do on a daily basis. This includes the internal organisation of large transnational NGOs, such as CARE, OXFAM, and Médecins Sans Frontières, all of whom rely extensively on email to manage their distributed network of employees, volunteers and complex missions. It includes the networking that takes place among different NGOs worldwide, who depend on ICTs to coordinate and strategically develop joint campaigns. ICTs are employed by NGOs and civic groups to orchestrate massive public protests and demonstrations, which have become an increasingly visible and, some would argue, important component of civic activism.[70] They are utilised for putting pressure on politicians and state bureaucrats directly, as in mass email petitions. And they increasingly play an important role in 'getting their message' out to a wider audience, and disseminating alternative news and media.[71]

Given the importance that ICTs present for civic networks, it is surprising that there is very little theorisation or examination of how it should be, or even presently is, configured. Works on global civil society often do little more than allude to the 'speed' of modern

---

69. For extended analysis, see Ronald J. Deibert, 'Civil Society Networks in an e-Connected World', in *The e-Connected World: Risks and Opportunities* ed. Stephen Coleman (London: McGill-Queen's University Press, 2003), 107-22.

70. See Jennifer Lee, 'How the Protestors Mobilized', *New York Times* (23 February 2003); and Cynthia Webb, 'Mobilizing Online Against War', *Washington Post* (11 March 2003) for overviews of how the Internet has played a central role in the mounting of unprecedented worldwide simultaneous protests of millions of citizens against the war on Iraq.

71. See Ronald J. Deibert, 'International Plug n' Play: Citizen Activism, the Internet, and Global Public Policy', *International Studies Perspectives* 1, no. 3 (2000): 255-72.

communications, or their capacity to cross vast distances.[72] The media itself is left untheorised or taken for granted. Practitioners fare not much better. Many NGOs contacted in the course of my research have expressed little knowledge of and interest in Internet security issues. This lack of attention to their very own material infrastructure may be a result of the overarching concern, both theoretically and practically, with the role of 'ideas' and 'norms' in advancing the causes that civil society actors hold.[73]

An entirely opposite problem afflicts those who are most intimately connected to the technology. Hackers, computer scientists, programmers, and electronic engineers closely associated with the evolution of the Internet know all too well the way in which its operating architecture cannot be assumed away as insignificant, for they are the very ones who have shaped and modified its evolution. Though rarely theorised as such, programmers have a primary grasp of the main principles of the media ecology theories developed by Harold Innis, Marshall McLuhan, and others: communication technologies are not mere empty or transparent vessels but they play a vital role in facilitating and constraining what can be communicated. From hieroglyphics to software, information is wrought and warped by the media through which it is conveyed. In today's hypermedia environment, such constraints have their effects through the dense layers of overlapping and interconnecting codes and programs that only coders and hackers can truly fathom.

Computer hacking has almost as long a history as do modern NGOs.[74] From the first prototypes employed in encryption cracking during the Second World War, computer technology has attracted

---

72. The collected volume by Thomas Risse-Kappen (ed.) *Bringing Transnational Relations Back in: Non-State Actors, Domestic Structures and International Institutions* (Cambridge: Cambridge University Press, 1995) has no reference in the index to 'communication', 'technology', or 'information'. Likewise, Margaret Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998) make only passing reference to communication and information technologies.

73. The anti-materialism of recent constructivist work, which forms the primary backdrop for most of the scholarship on civic networks, may explain the disregard of communication technologies. Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999) regards technologies as mere 'rump' material factors.

74. For a good historical overview, see Stephen Levy, *Hackers: Heroes of the Computer Revolution* (Garden City, NY: Anchor Press/Doubleday, 1984).

devoted enthusiasts and programmers.[75] The term 'hacking' today conjures up images of criminality and terrorist activity, largely due to the use of the term by law enforcement, defence, and intelligence agencies. But it did not always have such felonious associations. It is likely that the term has its origins in the Massachusetts Institute of Technology's Artificial Intelligence laboratory, where a large group of technically proficient programmers and engineers coalesced in the 1960s.[76] A hacker culture began to flourish widely with the development of ARPANET and the connection to the early Internet of computer science departments and other academic nodes around the world. As the Internet expanded, so too did the number and sophistication of hackers. Many informal hacker groups sprouted, occasionally meeting at large international conferences. DefCON, an annual meeting of defence contractors held in Las Vegas, Nevada, has become the most visible and arguably the largest conference of hackers, though others exist as well.[77]

While their campaigns for various technological protocols, privacy, and encryption regulations evince a clear normative direction, very rarely do they extend upwards and outwards to encompass a global political theory as a whole. Until recently, hacker culture has tended to be almost purely apolitical. There has been no distinct politics of hacking per se.[78] In part, this can be explained by the apolitical biases of the computing and engineering professions. Computer scientists — understandably — tend to be mired in the details of systems and codes instead. Though certainly not insignificant, their work in these areas is largely sub-structural and thus distinct from those of the civil society groups supported above. At best, a kind of unrefined libertarianism has pervaded hacker culture — a legacy of the west coast Californian roots of a large portion of early Internet development.[79] Historically, this

---

75. A good history of computer technology enthusiasts with a focus on the early development of the Internet is found in Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon & Schuster, 1996).

76. See Eric Raymond, *The Cathedral and the Bazaar* http://www.tuxedo.org/~esr/writings/cathedral-bazaar/.

77. See http://www.defcon.org/. As DEFCON has grown more popular, hackers have gravitated to other, less well known venues, such as CODECON, http://www.codecon.org/.

78. For discussion, see Douglas Thomas, 'The Politics of Hacking', *Online Journalism Review* (16 September 1998) http://www.ojr.org/ojr/technology/1017969411.php.

79. The entry for 'politics' in the popular *New Hacker's Dictionary* describes hacker politics as being, 'vaguely liberal-moderate, except for the strong

ideological outlook has rarely translated into concerted political action beyond support for unencumbered networks, strong encryption, and freedom of speech.

Cyclonic Interaction and Hacktivism[80]

The Canadian economic historian Harold Innis once described the contingent effect of social forces and technology environments coming together fortuitously to complement and reinforce each other as a kind of 'cyclonic' interaction.[81] Separately, or in different contexts, the social forces would have less of an impact. But in particular contexts and circumstances in which they are linked, they come together and erupt onto the political landscape having a force combined beyond their separate strengths.[82]

Such cyclonic interaction can now be seen occurring among citizen networks and hackers. Citizen networks are becoming more technologically sophisticated with an increasing reliance on computer networks and other ICTs. Hackers, on the other hand, are becoming increasingly politicised. While it may be optimistic in the extreme to hope that these cyclonic forces will be powerful enough to sweep aside the combined forces of security and commercial interests now increasingly governing the Internet, it is at least evidence of an embryonic contrary force, perhaps even an 'epistemic community' of sorts.[83]

libertarian contingent which rejects conventional left-right politics entirely. The only safe generalization is that hackers tend to be rather anti-authoritarian; thus, both conventional conservatism and "hard" leftism are rare. Hackers are far more likely than most non-hackers to either (a) be aggressively apolitical or (b) entertain peculiar or idiosyncratic political ideas and actually try to live by them day-to-day.' http://www.logophilia.com/jargon/jargon_59.html.

80. The following section draws from Ronald J. Deibert, 'Deep Probe: The Evolution of Network Intelligence', *Intelligence and National Security* (forthcoming, 2004).

81. See Harold A. Innis, *Empire and Communication* (Toronto: University of Toronto Press, 1950).

82. I have always found the notion of contingency, as expressed variously in Darwin's evolutionary theory, the philosophical pragmatism of William James, John Dewey, and Richard Rorty, and the science fiction of H.G. Wells, Philip K. Dick, and Robert Heinlen, among others, a major factor in social change; but one that very few IR theorists have appreciated or explored fully. See Richard Rorty, *Contingency, Irony, Solidarity* (Cambridge: Cambridge University Press, 1989).

83. The original notion of epistemic communities had much to do with scientific expertise, which I always thought was an unnecessary limitation of the model that more broadly refers to communities of knowledge and practice, as it is employed here. For discussions of 'epistemic communities', see Ernst B. Haas, *When Knowledge is Power: Three Models of Change in International Organizations* (Berkeley, CA: Berkeley University Press, 1991).

Formal organisation is good evidence that some concerted action is being undertaken and here the evidence is beginning to accumulate. Several dozen NGOs have emerged over the last several years with a mandate to influence the global communications policy agenda from a civil society perspective. Some of these, such as the Association for Progressive Communications (APC), have a long history of combining civil society interests with concerns about ICTs, and have a major global presence.[84] Others have emerged out of their own narrowly defined interests to begin to address broader shared concerns of ICT governance. Examples of the latter include Privacy International, the Electronic Privacy Information Center, and Computer Professionals for Social Responsibility from the privacy and computer security areas. Humanitarian and human rights NGOs, like Human Rights Watch, have developed similar extensive ICT policy agendas, as have civic activist networks in areas such as independent and community broadcasting and journalism. Reporters Without Borders, for example, has established an annual report on Internet policy that aims to raise awareness about some of the sea changes that have occurred in Internet governance over the last several years.[85] Though coming at the problem from different backgrounds, these groups are beginning to network around a shared agenda of communications security and privacy, freedom of expression, equal access, the protection of a vital public domain of knowledge, and the preservation of cultural diversity. Such networking is not merely accidental either. Major foundations, such as the Ford Foundation, Markle Foundation, and George Soros' Open Society Institute, have supplied critical funding and encouragement to bring civil society actors interested in information and communication technologies together.

Of course it's one thing to form a policy network; it is another to influence the policy agenda. Here the rubber hits the road, so to speak, and so far these groups have been unable to gain much traction. The main issue concerns the relative openness to civil society of the major international forums through which these groups' interests could be collectively articulated and acted upon. The World Intellectual Property Organization counts 179 nations as member states and is home to over 29 international treaties dealing with intellectual property, but it naturally sees private businesses and not civic networks or NGOs as its main clientele. State law enforcement and intelligence officials have been the primary architects of the EU Cybercrime Convention, with privacy officials and advocates left buzzing noisily around the process in a

84. http://www.apc.org/.

85. See Reporters Without Borders, *The Enemies of the Internet* http://www.rsf.org/ennemis.php3#.

despair-filled funk. The main regulatory body in charge of management of the Internet's root architecture, The Internet Corporation for Assigned Names and Numbers (ICANN), has come under fire for being dominated by the United States and for some of its undemocratic processes, but the stakes are too big, the sunk costs too high, and the alternatives too uncertain to change its governing structure.[86]

Perhaps most representative of the frustrating lack of access that civic networks face in policy forums is the World Summit on the Information Society (WSIS), headed by the International Telecommunications Union (ITU).[87] The WSIS is a two-phase UN summit scheduled for December 2003 in Geneva and 2005 in Tunisia. The ITU has the lead role as organiser of the WSIS, whose stated aim is 'to develop a common vision and understanding of the Information Society, to better understand its scope and dimensions and to draw up a strategic plan of action for successfully adapting to the new society.'[88] Although the WSIS process makes provisions for civil society participation, this has so far been frustrating. The usual problem of lack of funding and resource imbalances between states, corporations and civil society actors has decidedly skewed input into the process away from grassroots organisations and civil society organisations from the developing world. Many NGOs have also been left out of the consultative loop in the formulation of their own state's strategies, as governments sidle up to their usual industry colleagues with the largest stakes. Standing at the pinnacle of the WSIS is the problem of the ITU itself, which has had very little experience with civil society organisations due, among other reasons, to its pricey membership fees for non-state actors.

At the time of writing, the first phase of WSIS has been completed with most outside observers perceiving the process as a mixed success at best. Although somewhat marginalised in the formal process of the WSIS leading up to Geneva, civic networks themselves were positively catalysed by their extensive networking, producing an alternative declaration and what promises to be long-lasting working relationships.[89] Ironically, their marginalisation from the WSIS process may have been the most important factor contributing to the

---

86. For discussion, see http://www.icannwatch.org/ and Daniel Pare, *Who's Master of this Domain: Internet Governance in Transition* (Lanham, MD: Rowman & Littlefield Publishers, 2002); and Hans Klein, 'ICANN and Internet Governance: Levering Technical Coordination to Realize Global Public Policy', *The Information Society* 18 (2002): 193-207.

87. http://www.itu.int/wsis/.

88. Ibid.

89. As part of the Canadian civil society delegation myself at WSIS, I was struck by the extent to which civil society actors working around ICT issues had

development of a relatively cohesive transnational network. From their mutual interaction, ideas are already beginning to emerge that give policy and technology focus to global civic networks, including creating zones of civic-run Internet access points and 'overlay' networks designed to protect and preserve the public commons, creating a civil society capacity for directly monitoring corporate and state surveillance and censorship, and finding alternative ways to enhance connectivity for civil society actors in the developing world, among others.[90]

Hacktivism

Of course, problems of access to policy forums for civil society organisations are not unique to the ICT sector. But, one area where civic networks may have the upper hand that civil society organisations working in other policy sectors do not is in terms of the influence on the very environment of the Internet itself. Since its beginnings, the Internet's architecture has been shaped not only by states and corporations but also by the distributed base of users themselves. Indeed, networks of skilled individuals have been responsible for some of the most revolutionary Internet technologies, from open source/free software platforms to P2P networks and encryption systems. The Internet's saving grace may lay in the resources of its millions of users spread around the world, especially as those networked individuals harness their creativity to politically defined goals. Having been turned on and energised by the distributed potential of digital-electronic communications, these skilled individuals and groups are almost impossible to turn off.

The term used to describe this combination of politically motivated, grassroots technology development is 'hacktivism'.[91] Inspired by the original definition of the term hacker, 'exploring the details of

become a major cohesive force. Again, the presence of major foundations, such as Ford and the Open Society Institute, was a major factor.

90. An excellent overview can be found in Sean O Siochru, *Global Governance of Information and Communication Technologies: Implications for Transnational Civil Society Networking* (Social Science Research Council Report, November 2003).

91. For a different interpretation of hacktivism, see Dorothy Denning, 'Activism, Hacktivism, and Cyberterrorism', Paper prepared for the Nautilus Institute, December 1999 http://www.nautilus.org/info-policy/workshop/papers/denning.html. While I find the empirical portion of Denning's article illuminating, her definition of hacktivism is misleading, employing the typical law enforcement practice of associating hacking with criminal activities — an association that not only ignores the history of hacking but the positive potential of hacking as a tool for legitimate citizen activism. I prefer the term 'cracking' for criminal activities directed at or through computer networks.

programmable systems and how to stretch their capabilities',[92] hacktivists have developed technologies in three key areas: anti-censorship and freedom of speech, privacy, and Internet security. Some of these technologies are developed by ad hoc groups of hackers and activists, others by small companies. The scope of these technologies ranges from small, simple scripts and programs to highly developed P2P network protocols, steganography tools, and advanced software development. Hacktivists gather around major Internet forums, like Slashdot, monitoring policy developments and offering technical solutions.[93]

One of the more interesting hacktivist groups is Hacktivismo, an offshoot of one of the Internet's oldest and most well known hacker groups, the Cult of the Dead Cow.[94] Hacktivismo may at first appear to be a typically sophomoric club of computer enthusiasts, but closer inspection reveals a more serious agenda. Hacktivismo's Declaration takes as its starting point the principles and purposes enshrined in Article 19 of the Universal Declaration of Human Rights regarding freedom of speech. Its board of advisers includes a high profile human rights advocate and renowned Internet lawyer. But it is the network of technology programmers that gives Hacktivismo its clout and credibility. In recent years, Hacktivismo has been responsible for several privacy and security enhancing technologies designed to allow citizens in repressive states to surf around censorship and surveillance.[95] Hacktivismo is by no means alone. Hacktivist tools have sprouted all over the Internet in increasing numbers, and increasingly with the financial support of major international foundations. With nearly every government attempt to censor online communications, hacktivists create and distribute tools to get around them. As soon as a corporation comes up with the latest method of protecting digital copyright, hacktivists are there to crack the code. Although this movement is still multi-directional and politically immature, it can be seen as a potentially formidable check on attempts to re-exert control over the Internet's distributed, open architecture.[96]

---

92. http://www.jargon.8hz.com/jargon_23.html#SEC30.
93. http://www.slashdot.org/.
94. http://www.hacktivismo.com/.
95. For an overview of these technologies, see the Citizen Lab's OpenNet Initiative http://opennetinitiative.net/.
96. Although space prevents it, a more thorough discussion of the free software/open source movement would be warranted in this context. Basically, free software/open source refers to the global network of programmers who work jointly on software projects whose code is not proprietary. A major challenge to existing intellectual property regimes, and riven by internal

Conclusion

Generally speaking, theories of globalisation, global civil society, and transnational networks have assumed a continuing trajectory of increasingly open and distributed communications. This in turn is gradually diminishing the power of the state while fuelling the rise of what James Rosenau aptly called 'sovereignty-free actors'. As the analysis above suggests, that assumption can no longer be taken for granted. Although the properties of the Internet may very well have been biased towards openness and decentralisation in the past, it is important to remember that the Internet is not a fixed medium that will remain unchanged into the future and as it changes, so too will its consequences. The Internet is, rather, a complex mix of technological systems in constant evolution, morphing in response to the pressures and technological choices of powerful actors able to influence its overall architecture.[97] States — especially powerful ones like the United States — still constitute one of those major actors.

For those concerned with deepening and expanding the prospects for global democratic governance and the flourishing of global civil society in the context of an emerging single world polity, the evolving nature or architecture of the communications infrastructure should be, therefore, of vital concern. For all its many faults and digital divides, it is the Internet that is providing the means by which an increasing number of citizens around the world can and will deliberate, debate, and ultimately have an input into the rules of the game by which they are governed. While at one time the Internet, and in particular its characteristically liberal environment, could be taken for granted by civil society actors, that time has now passed. A formidable set of social forces is pushing regulations and technologies that, whatever their individual aims, collectively have the effect of taking that open, liberal architecture in a decidedly different direction. Global citizen networks must now become dynamic participants in the politics of Internet design, or risk having the power source for their activities increasingly unplugged.

To do so, however, IR theorists — interested in and normatively in favour of opening up spaces for alternative voices, grassroots

disputes itself, the free software/open source movement could be one of the most important constitutive elements of a communications infrastructure oriented around principles partial to global democracy, and freedom of speech and communications. See Steven Weber, *The Success of Open Source* (Cambridge, MA: Harvard University Press, 2004).

97. For an analysis of the relationship between privatising dynamics and accountability on the Internet, see Saskia Sassen, 'Digital networks and the state: some governance questions', *Theory, Culture and Society* 17, no. 4 (2000): 19-33.

democracy, and global democratic governance to flourish — will have to pay greater attention to the material foundations upon which global communications take place. Doing so means qualifying notions of 'ideas all the way down' and 'worlds of our making' to acknowledge the extent to which material factors of communication, albeit socially constructed,[98] present a formidable set of real constraints on the realm of the possible.[99] Quite naturally, those interested in such topics have been concerned primarily with moving away from older positivist-materialist notions of state interaction to concerns about the circulation of ideas, the framing role of discourses, and processes of legitimation. But communication does not take place in a vacuum. It is anchored within and shaped by the material properties of the communications environment.

It is with some small measure of optimism then that one can look upon recent developments in the area of civic networks and Internet governance. Among the converging interests of NGO users, privacy advocates, computer scientists, and grassroots media, one can detect the emergence of a kind of 'epistemic community'. Although principles have nowhere been formally codified, a constellation of values brings these groups together to help give shape to a common agenda. Bolstering this transnational social movement is the powerful ammunition of politically motivated research and development of civic technologies that feed into, and give concrete shape to, the Internet's basic structural design. Those material constraints, embedded in code, may in the long run provide the most important constitutional mechanisms to ensure that a communications infrastructure supports, rather than detracts from, the ongoing project of global democratic governance.

Ronald Deibert is Associate Professor of Political Science and Director of The Citizen Lab, Munk Centre for International Studies, University of Toronto

---

98. Wiebe Bijker, Thomas Hughes, and Trevor Pinch, (eds.), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge: Cambridge University Press, 1987).

99. I have thought, in this respect, that the notion of 'cyberspace' is misleading and counterproductive. It suggests a distinct realm, separate from the materiality of 'real space' or 'meatspace' as it is often referred to by Internet enthusiasts. Much like geography went through a transition from abstract Cartesian notions of 'space' to better understand local varied conditions of 'place', those who study the Internet need to think it of less in terms of a virtual abstract environment and more for what it really is — a complex network of codes, programs, routers, firewalls, fibre optic cables, frequency spectrums, satellites, and so on. Doing so will highlight not only material constraints that the communication environment imposes, but methods of control and authority, many of which are buried within the subterranean layers of the network.