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

Ronald J. Deibert,
Associate Professor of Political Science
Director, The Citizen Lab
Munk Centre for International Studies
University of Toronto
1 Devonshire Place, Toronto, Ontario, M5S 3K7 Canada
Tel: (416) 946-8916 Fax: (416) 946-8915
E-mail: r.deibert@utoronto.ca
http://www.citizenlab.org

Version 1.0, February 9, 2003
Prepared for the International Studies Association Conference, Portland, Ore

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

1.0 Introduction

One way to think about "globalization" is to equate it with a specific ideology and set of social forces that are transforming the world political economy in the direction of hyper-liberalism.[1] This particular conceptualization sees globalization emerging only in the latter half of the twentieth century with the end of Bretton Woods and the shift to neo-liberal principles worldwide, driven largely by private corporations, the major industrialized states, and the principal international organizations that manage the world economy, such as the World Bank and the I.M.F. Although this conceptualization is probably the most widely shared among both opponents and adherents, it is not the one adopted in this paper.

In this paper, I define globalization as a much deeper world historical process tied to hundreds of years of industrialization and centuries of technological change in communication and transportation capabilities which have irreversibly brought once isolated and loosely integrated political communities into intensive proximity on a planetary scale.[2] While these processes have not yet created a single world state, they have set the parameters for a single world polity, albeit one that contains an uneasy mix of persistent elements of the old "Westphalian" sovereign state system and new forms of global governance. Debates about "private authority," "neo-medievalism," "pooled sovereignty" and the "legitimacy of global governance" are all, from this perspective, symptomatic expressions of the difficult transition to and working out of the scale-shift to politics in a single global village.[3] From now on, it is all world domestic politics.

Like a growing number of others who take this scale-shift as a first premise, I am principally concerned with doing research and articulating ways to help shape this

---

[1] See, for example, Saskia Sassen, *Globalization and its Discontents*, (New York, The New Press, 1998); Mark Neufeld, "Globalization and the Re-Definition of Democratic Governance: From Compensatory to Protective Democracy," *TIPEC Working Paper 01/7* found online at: http://www.trentu.ca/tipec/neufeld7.pdf; and James H. Mittleman, (ed.), *Globalization: Critical Reflections*, (Boulder: Lynne Reinner, 1996).

[2] Daniel Deudney, *Bounding Power: Geopolitical Change, States Systems, and Republican Restraint*, (forthcoming: Princeton University Press).

[3] For private authority, see Rodney Bruce Hall and Thomas J. Biersteker, (eds.) *The Emergence of Private Authority in Global Goverannce*, (Cambridge: Cambridge University Press, 2003); for neo-medievalism, see Ronald J. Deibert, "*Exorcismus Theoriae*: Pragmatism, Metaphors and the Return of the Medieval in IR Theory," *European Journal of International Relations*, (Vol. 3, No. 2, June 1997): 167-192. For pooled sovereignty see Robert O. Keohane and Stanley Hoffman, "Institutional Change in Europe in the 1980s," in *The New European Community: Decision-making and Institutional Change*, edited by Keohane and Hoffman. (Boulder, Co: Westview Press, 1991). On "legitimacy and global govenance, see Steven R. Bernstein, *The Compromise of Liberal Environmentalism*, (NY: Columbia University Press, 2001).

embryonic world polity in the direction of global liberal democracy.[4] My own empirical focus within this backdrop is on information and communication technologies (ICTs), and in particular on how the Internet and other telecommunications media ought to be secured and designed to best facilitate those goals.

Here, the current realities and future prospects are mixed. On the one hand, the Internet has provided a means through which citizens from around the globe can communicate and deliberate in a speedy and relatively open fashion. It has been the vehicle for a remarkable flourishing of citizen-to-citizen communications on a global scale and the proliferation of individual expression through web publication, all of which would be essential for the future of global democratic discourse. On the other hand, however, a confusing mix of private and public ownership structures criss-crossing several major international regimes presently governs the Internet. The vast majority of people on the globe have no access to it. And, most importantly, the architecture of the Internet is fast transforming away from its original open, distributed design as it becomes more intensively regulated.

These questions of the politics of Internet security and design have taken on a new urgency in the wake of September 11th and the ensuing global war on terrorism. As will be described below, legislation has been passed in virtually every industrialized country 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.

The intent of this paper is to provide an overview of the current state-of-play with regard to these new pressures as well as to lay out some of the principles and practices that I see as essential to its evolution if it is to eventually provide the foundations for a global liberal-democratic world order. Mostly this is a rather pessimistic story. If we start from any ideal perspective on what the communications infrastructure should look like for global democratic governance (and indeed there is substantial variation here) 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 democratic communications become increasingly fragile. The second half of this paper outlines the prospects for contrary forces emerging to censorship, surveillance, and militarization. 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

[4] See in particular David Held, *Democracy and the Global Order,* (Stanford: Stanford University Press, 1996); Daniele Archibugi and David Held, (eds.) *Cosmopolitan Democracy: An Agenda for a New World Order*, (Oxford: Blackwell, 1995); and Richard Falk, *A Study of Future Worlds*, (London: MacMillan, 1975).

transnational paradigm of Internet security and design, oriented around shared values and technologies. But their challenges are formidable.

2.0 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. 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.[5]

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."[6] 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.[7]

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.[8] 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,[9] 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

---

[5] For representative views, see John Perry Barlow, *A Declaration of the Independence of Cyberspace*, (February 1996), found online at: http://www.eff.org/~barlow/Declaration-Final.html; and George Gilder, *Telecosm*, (NY: Free Press, 2000).

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

[7] See also Audrey N. Selian, "ICTs in Support of Human Rights, Democracy, and Good Governance," *International Telecommuications Union*, (August 2002).

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

[9] See, for example, Deibert, *Parchment, Printing, and Hypermedia*, Harold Innis, *Empire and Communication*, (Oxford: Oxford University Press, 1952); Marshall McLuhan, *Understanding Media* (NY: McGraw Hill, 1964).

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

2.1 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.[10] 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 widely 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 in section 2.3 below. A more unlikely source comes from intensifying pressures to regulate intellectual property and copyright, to which we now turn.

2.2 Commercial Censorship

As information has become increasingly digitized, so have a wide range of consumer products, including movies, music, and books. Although entertainment, software, and other commercial industries have sought to capitalize 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. Once digitized and placed on distributed networks, information is easy to duplicate and distribute. Companies and their lobbyists in the affected industries, such as the RIAA and MPAA, have claimed large losses in potential sales, though determining figures with precision rests on questionable counterfactuals.[11] 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 organization Business Software Alliance (BSA).[12]

---

[10] 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"

[11] The Recording Industry Association of America and the Motion Picture Association of America.

[12] See the *Seventh Annual BSA Global Software Piracy Study* (June 2002), found online at: http://www.bsa.org/usa/policyres/admin/2002-06-10.130.pdf

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.[13] 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 Millenium Copyright Act* (DMCA), an act of US Congress that was signed into law on October 28th, 1998, by President Clinton, and whose purpose is to update U.S. copyright laws for the digital age.[14] According to a study by the Electronic Frontier Foundation on the *Unintended Consequences of the DMCA*, the Act has been employed as a tool of anti-competition, has stifled legitimate research into cyber-security and encryption technologies, and has undermined "fair use".[15] To give just a few egregious examples, a garage door opener company has employed the DMCA to prevent rival companies from developing universal remote controls that operate on its system.[16] 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.[17] 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.[18]

---

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

[14] Full text of the Act is found here: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf

[15] *Unintended Consequences: Three Years Under the DMCA*, Electronic Frontier Foundation (May 3, 2002), found online at: http://www.eff.org/IP/DMCA/20020503_dmca_consequences.pdf

[16] For references, see "DMCA vs. Garage Door Opener," at Politech, http://www.politechbot.com/p-04319.html

[17] Jonathan Band, "Congress Unknowingly Undermines Cyber-Security," *SiliconValley.Com* (December 16, 2002), found online at: http://www.siliconvalley.com/mld/siliconvalley/4750224.htm?template=contentModules/printstory.jsp

[18] 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, November 9-11, 2001. This paper and others from the conference can be found online at: http://www.law.duke.edu/pd/papers.html#history

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*,[19] that would grant copyright holders near-immunity from the law while using denial of service attacks against computers that are suspected of trading illegally copyrighted material over peer-to-peer (P2P) networks -- a startling legitimization of cyber-vigilantism. Berman is expected to re-introduce a revised version of the bill in the 108th session of the Congress. Other legal measures have targeted Internet Service Providers (ISP), holding them accountable for traffic that flows through their networks.[20] By imposing the responsibility to monitor traffic to the ISP level not only does such legislation blur 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 internationalized through similar legislation being adopted in other countries. The United States Trade Representative has pushed the *DMCA* in bilateral trade negotiations[21], and many of its main elements are manifest in treaties administered by the World Intellectual Property Organization (WIPO). Among other things, the internationalization 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 encourage 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.[22]

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.[23] 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 centralized 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.

---

[19] http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.05211

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

[21] For one example, see Simon Hayes, "US Tightens Net Copyright," *News.Com.Au*, (January 28, 2003), found online at: http://www.news.com.au/common/printpage/0,6093,5896759,00.html

[22] 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(1, 1998)*.

[23] See *No Competition: How Monopoly Control of the Broadband Internet Threatens Free Speech*, (An ACLU White Paper), found online here: http://archive.aclu.org/issues/cyber/NoCompetition.pdf

Cable Internet access providers can and often do control the overall speed of a customer's connection, 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 ACLU report noted, the latter is "like a phone company being allowed to own restaurants and then provide good service and clear signals to customers who call Domino's and frequent busy signals, disconnects, and static for those calling Pizza Hut."[24] 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 most concerning are measures taken to protect intellectual property and copyright through technical means, and in particular through the introduction of codes built into the software and hardware that structure permissible communications.[25] Microsoft's *Palladium* 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.[26] More broadly, such initiatives foment a litigious environment around electronic communications that in turn could lead to self-censorship. You know something doesn't 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.[27]

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 –written into the very architecture of the Internet itself, in other words.[28] Such a shift in intellectual property regimes would not just affect a compartmentalized sphere of activity on the Internet. It would not just ensure that piracy is stemmed (although even that is debatable in a digital environment). It would affect the

[24] *Ibid*.
[25] An extended discussion can be found in Lessig, *Code*.
[26] See Hal R. Varian, "New Chips Can Keep a Tight Rein on Consumers," *New York Times*, (July 4, 2002).
[27] 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*, (January 18, 2003). The New York Supreme Court struck down the policy as unconstitutional.
[28] Lessig, *Code*.

very architecture of the Internet itself, 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.

2.3 State Censorship

One of the conventional wisdoms about the Internet outlined earlier is that states cannot control Internet communications. 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.[29] While global flows of communication have made state censorship difficult, to be sure, it has 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.[30] 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.[31]

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 organizations have issued lengthy descriptions of Internet and other media censorship, some of which have evolved into regular annual reports.[32] However, empirical knowledge of Internet censorship is still very much in is infancy.[33] 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.

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 Café's), and a national firewall at the Internet backbone level

---

[29] See, for example, Walter Wriston, *The Twilight of Sovereignty*, (NY: Scribner, 1992).

[30] 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), found online at: http://www.cmis.csiro.au/projects+sectors/blocking.pdf

[31] For overviews, see Human Rights Watch, *Freedom of Expression on the Internet*, Annual Report 2000, found online at: http://www.hrw.org/wr2k/Issues-04.htm, and Reporters Without Borders, *Enemies of the Internet*, found online here: http://www.rsf.org/ennemis.php3

[32] See footnote 27 above, and the OpenNet Initiative at http://oni.citizenlab.org/ for more details and reports.

[33] See Jonathan Zittrain and Benjamin Edelman, "Documentation of Internet Filtering Worldwide," Berkman Center for Internet and Society, Harvard Law School, for empirical research on China and Saudia Arabia that complements the research outlined in this paper, found online here: http://cyber.law.harvard.edu/filtering/

designed to block access to Internet content deemed "undesirable" or "subversive."[34] Although it is known that China employs content filtering, little is known about what or how much, precisely is being blocked, which is a state secret. A study undertaken under the direction of the author analyzed 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 (See Appendix A: Project C). The results indicated not only that 20% 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.

Some of the more aggressive content filtering systems have been adopted in Islamic regimes. While these countries admittedly block access to pornographic sites, they have also begun to employ the same filtering technologies to block political websites, particularly human rights websites critical of their regimes' records.[35]

Saudia 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 Minister's 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."[36] 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 Yemem, among others.

Many other developing countries have also modeled 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

[34] For extended discussion, see Ronald J. Deibert, "Dark Guests and Great Firewalls: Chinese Internet Security Policy," *Journal of Social Issues*, (2001) 58, 1: 143-158.
[35] The following research draws on the reports and studies outlined in previous notes, as well as empirical research undertaken at the Citizen Lab through the Internet Censorship Explorer (ICE), found here: http://oni.citizenlab.org/oni/ice/
[36] See Human Rights Watch, *Freedom of Expression on the Internet*, Annual Report 2000, found online at: http://www.hrw.org/wr2k/Issues-04.htm

have documented a tightening grip over media recently, including the Internet. Independent media in Indonesia and Malaysia that benefited by liberalization 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 licenses 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.[37] Although our research has only established some initial findings in countries other than China, using technical means we have so far determined that Internet filtering technologies have been used in Singapore, Vietnam, and Myanmar (Burma) to bloc political sites.[38]

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. 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 NGO's and civic networks with other domestic and international NGO's by effectively blocking email access, websites and other Internet services.

3.0 Electronic Surveillance

An important lever of 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, United Kingdom, Australia and New Zealand.[39] 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 centralization 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, the United States Patriot Act, and the United Kingdom Crime and Security

---

[37] See Alan Boyd, "Dark Days for Asian Journalism," *Japan Today*, (February 1, 2003), found online at: http://www.japantoday.com/e/?content=comment&id=330

[38] See the Internet Censorship Explorer (ICE) at http://oni.citizenlab.org/oni/ice/ for expanded details on our research in this area.

[39] Bamford, *Body of Secrets*.

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 states outside of Europe as well, such as Canada, Australia, and the United States, all of whom have signed on to it making domestic adjustments to its invasive provisions. 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."[40] Although each of these pieces of legislation differ, what they share 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.[41]

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.[42]

The surveillance system that has generated the most alarm among privacy advocates is 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 are fuzzy, early reports indicate 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.[43] 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 web site. At the time of writing, the U.S. Congress has frozen the budget for the TIAO, and there are plans to revise it with some limited

[40] 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 U.S. origin, the CALEA essentially internationalizes US surveillance regulations in practice.

[41] Such regulations have not been limited to the northern industrialized countries. In the immediate aftermath of 9.11, for example, several Central Asia 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.

[42] Mark Townsend and Paul Harris, "Security Role for Traffic Cameras," *The Observer*, (February 9, 2003), found online at: http://www.observer.co.uk/politics/story/0,6903,892001,00.html

[43] See Lauren Weinstein, "Year In Privacy: Citizens Lose," *Wired*, (December 30, 2002), found online at: http://wired.com/news/privacy/0,1848,56954,00.html

oversight.[44] 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 organizations have been undertaking analogous surveillance practices targeting consumer purchasing and transaction habits both on and offline. From the use of "cookies" to track Internet surfing 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. A report by the American Civil Liberties Union noted with alarm that the new surveillance regimes being imposed in the United States "will place millions of innocent Americans under government scrutiny in an epidemic of privacy invasions." In spite of these and many other pleas, the shocks of 9.11 have seemingly 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, will of course be 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.

4.0 Militarization of Cyberspace

Accompanying electronic surveillance has been the largely undebated militarization 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. 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. 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

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

destruction, threats from terrorist actors employing the Internet appear to bode little more than periodic disruptions to Internet traffic.[45]

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. Theory has definitely trailed behind practice in this case.

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 organizational structures related to them, from advanced computing and communications technologies to remote sensors. Going back further, its roots can be found in the use of propaganda and psychological warfare techniques and electronic jamming that date to World War II, 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.[46] The United States' military now openly employs computer hackers, develops advanced Trojan horses, viruses, and worms, and has used techniques of cyber-propaganda leading up the conflict in Iraq.[47]

It is not alone. Dozens of countries around the world have either debated or adopted offensive cyber war capabilities, including China, Russia, Taiwan, and the United Kingdom, Australia, and Canada. The number of documented state cyber war has risen in recent years as well. In spite of the greater penetration of these technologies in advanced industrialized countries, many of the more prominent examples of information warfare have occurred in the developing world.[48] 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.[49] During the Russian campaign against Chechnya in the mid-1990s, Chechnyahn commanders made efficient use of cell phone networks and eavesdropped on insecure Russian radio networks to organize devastatingly successful military strikes. In 2000, an "inter-fada" erupted between Israeli

[45] Steve Alexander, "Some Experts Say Cyberterrorism is Very Unlikely," *Star Tribune*, (February 13, 2003), found online at: http://www.startribune.com/stories/535/3650296.html
[46] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, (February 7, 2003).
[47] See Dan Caterinicchia, "DOD Plans Network Attack Task Force," *Federal Computer Week*, (February 7, 2003), found online at: http://www.fcw.com/fcw/articles/2003/0203/web-net-02-07-03.asp
[48] This section draws from Rafal Rohozinski, "Bullets to Bytes: Reflections on ICTs and "Local" Conflict," in Robert Latham, (ed.) *Bombs, Bytes, and Bandwidth*, (forthcoming: New Press, 2003).
[49] See *Ibid*.

and Lebanonese 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, 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.[50]

What are the concerns for global civic networks of the militarization of cyberspace? In some respects, the threats may be overdrawn. Just as networked redundancies and distributed security practices constrain the potential ramifications of cyberterrorism, 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 who are home to private corporations with assets spread transnationally throughout the globe face strong financial incentives to preserve the security and seamless functioning of global communication 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 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 militarization 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? Though not described in terms of arms control *per se*, the following section offers a survey of the prospects.

5.0 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 over the last twenty years, changes to the Internet 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 state military and intelligence agencies on the other.[51] Unless a new transnational social movement arises to bring to bear on

[50] See *Ibid.*

[51] For an extended discussion, see Ronald J. Deibert, "Circuits of Power: Security in the Internet Environment," in J.P. Singh and James N. Rosenau, (eds.) *Information Technologies and Global Politics: the Changing Scope of Power and Governance*, (NY: Suny Press, 2002), pp. 115-142.

Internet governance issues the concerns of civil society actors, the prospects of building a communications infrastructure for global democratic governance will become increasingly bleak. The remainder of this paper outlines some of the constraints and opportunities of such a social movement emerging, beginning with the two solitudes of civil society actors and information technology specialists.

5.1 Two solitudes

From local grassroots movements in rural Ontario to non-governmental organizations (NGOs) in the Zambia, ICTs, including the Internet, are the information infrastructure -- the material nerves – of civil society networks around the world.[52] 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 organization of large transnational NGOs, such as CARE, OXFAM, and Medecins San Frontiers, all of whom rely on email to manage their distributed network of employees, volunteers and complex missions. It includes the networking 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 civil society activism. They are utilized 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.

Given the importance that ICTs present for civic networks, it is surprising that there is very little theorization 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 communications, or their capacity to cross vast distances. The media itself is left untheorized or taken for granted. Many NGOs contacted in the course of my research have demonstrated surprising lack of knowledge and interest of 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.

An entirely opposite problem afflicts those who are most intimately connected to the technology. Internet activists and hackers, computer scientists, 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.

[52] For extended analysis, see Ronald J. Deibert, "Civil Society Networks in an e-Connected World," in Stephen Coleman, (ed.) *The e-Connected World: Risks and Opportunities*, (London: McGill-Queen's University Press, 2003), pp. 107-122.

Computer hacking has almost as long a history as do NGOs.[53] From the first prototypes employed in encryption cracking during World War II, computer technology has attracted devoted enthusiasts and programmers.[54] The term "hacking" today conjures up images of criminality and terrorist activity, largely due to the use of the term by law enforcement, defense, and intelligence agencies. But it did not always have such felonious associations. The term likely 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.[55] 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 defense contractors held in Las Vegas, Nevada, has become the most visible and arguably the largest conference of hackers, though others exist as well.[56]

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.*[57] 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.[58] Historically, this ideological outlook has rarely translated into concerted political action beyond support for unencumbered networks, strong encryption, and freedom of speech.

---

[53] For a good historical overview, see S. Levy Hackers: Heroes of the Computer Revolution, Anchor Press/Doubleday, Garden City, NY, 1984.

[54] 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 and Schuster, 1996.

[55] See Eric Raymond, The Cathedral and the Bazaar, found online at http://www.tuxedo.org/~esr/writings/cathedral-bazaar/

[56] See http://www.defcon.org/

[57] For discussion, see Douglas Thomas, "The Politics of Hacking," Online Journalism Review, (September 16, 1998) found online at http://ojr.usc.edu/content/story.cfm?request=70

[58] The entry for "politics" in the popular "New Hacker's Dictionary" describes hacker politics as being "Vaguely liberal-moderate, except for the strong 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." Found online at http://www.logophilia.com/jargon/jargon_59.html

5.2 Cyclonic Interaction and Hacktivism[59]

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 in what he described as kind of *cyclonic* interaction.[60] 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.

Such *cyclonic* interaction can now be seen occurring among civil society groups and hackers. Civil society groups are becoming more technologically sophisticated with an increasing reliance on computer networks. Hackers, on the other hand, are becoming increasingly politicized. 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 governing the Internet, it is at least a positive first step towards a contrary force.

Formal organization 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. 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. 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.

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

[59] For an extended discussion of the following section, see Ronald J. Deibert, "Deep Probe: The Evolution of Network Intelligence," *Intelligence and National Security*, (forthcoming, 2003).
[60] See Harold Innis, Empire and Communication, (Toronto: University of Toronto Press, 1950).

with intellectual property, but it naturally sees private business and not civil society as it main clientele. States' law-enforcement and intelligence officials have been the primary architects of the EU's Cybercrime Convention, with privacy officials and advocates left buzzing noisily around the process in a 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 money is too big of an issue at this point to allow genuine civil society input.[61]

Perhaps most representative of the frustrating lack of access that civic networks face in policy forums is the upcoming World Summit on the Information Society (WSIS), headed by the International Telecommunications Union (ITU). 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 Summit, 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."[62] Although the WSIS process makes provisions for civil society participation, the process 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 organizations and civil society organizations 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 organizations due, among other reasons, to its pricey membership fees for non-state actors. The first summit has not even begun and yet most observers expect the outcome of the WSIS to be partial to business and law-enforcement.[63] Some even anticipate a global version of the US Patriot Act to be the most likely result of the WSIS process.

5.3 Hacktivism

Of course problems of access to policy forums for civil society organizations are not unique to the ICT sector. But one area where civic networks may have the upper hand that civil society organizations working in other policy sectors do not is in terms of the influence on the very environment of cyberspace 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 platforms to p2p networks and encryption systems. The Internet's saving grace may lie in the resources of its millions of users spread around the world, particularly as those

[61] For discussion, see http://www.icannwatch.org/
[62] See http://www.itu.int/wsis/
[63] For discussion, see Sean O Siochru, "Civil Society Participation in the World Summit on the Information Society: Issues and Principles," *A Discussion Paper for Working Group 1 on Civil Society Participation in the WSIS*, found online here: http://www.comunex.net/wsis/docs/wg108c.pdf

networked individuals harness their creativity to politically-defined goals. Having been turned on and energized 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."[64] Inspired by the original definition of the term hacker, "exploring the details of programmable systems and how to stretch their capabilities", hacktivists have developed technologies in three key areas: anti-censorship, 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 peer-to-peer network protocols, stegonography tools, and advanced software development. Hacktivists gather around major Internet forums, like Slashdot, monitoring policy developments and offering technical solutions.[65]

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*.[66] Hacktivismo may at first appear to be a typically sophomoric club of computer enthusiasts, but a 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 advisors includes a high profile human rights advocate and renowned Internet lawyer. But it's 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.[67] *Hacktivismo* is by no means alone. Hacktivist tools have sprouted all over the Internet in increasing numbers. With 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.

---

[64] For a different interpretation of hacktivism, see Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism," Paper prepared for the Nautilus Institute, December 1999, found online at 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.

[65] http://www.slashdot.org/

[66] http://www.hacktivismo.com/

[67] For an overview of these technologies, see the Citizen Lab's OpenNet Initiative, found here: http://oni.ciitzenlab.org/

6.0 Conclusion

For those concerned with deepening and expanding the prospects for global democratic governance in the context of an emerging single world polity, the nature or architecture of the communications infrastructure is of vital importance. For all of its many faults, it is the Internet that to date is providing the means by which citizens around the world can 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 are 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.

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."[68] 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. But the battle has only just begun and the opposition has, at the present time, a much greater upper hand.

[68] For discussion of "epistemic communities," see Ernst B. Haas, *When Knowledge is Power: Three Models of Change in InternationalOrganizations*, (Berkeley: Berkeley University Press, 1991).

Appendix A: Project C
Lead Researcher Nart Villeneuve

About Project C
Project C is a *censorship enumeration* project that explores the relationship between censorship, technology and resistance through a technical analysis of state-imposed content filtering and blocking schemes illustrated through the identification of blocked URLs. Through this enumeration Project C aims to:

- Heighten public awareness of human rights, free speech and privacy issues
- Expose the relationship between censorship, surveillance and the state
- Explore the legal, political and economic dimensions of censorship
- Identify and challenge companies that profit from censorship technologies
- Highlight and support the growing resistance to Internet censorship that is occurring on the political, legal, and technological levels.

Project C: Round One
The initial focus of Project C is on national backbone Internet blocking in the People's Republic of China. 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 Café's), and a national firewall at the Internet backbone level designed to block access to Internet content deemed "undesirable" or "subversive".

This study analyzed Internet blocking at the 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. The primary focus of this study was CHINANET, which is the largest Internet Service provider in China.

When an Internet user requests content from behind the "Great Cyber Wall" the request is routed through a series of backbone network routers. The routers contain tables of banned Internet Protocol (IP) addresses and simply do not forward requests to the banned addresses thus denying the user access to the requested web content. The user will receive an error indicating that the request has failed but will not tell the user why the request has failed.

Figure 1 is a screenshot of a visual traceroute request from a server on CHINANET to the website of Human Rights Watch (www.hrw.org). The request originating in China is router (d?) through various regional routers from CHINANET's Beijing province network but the request is finally blocked at the CHINANET backbone network. The offending router in this case, p-1-0-0-r1-i-bjbj-1.cn.net (202.97.33.2), is manufactured by Cisco[69] , an American company that does considerable business with China. Cisco provides Internet backbone technology to the major Internet Service Providers in China.

[69] Enumeration scans performed on this router indicate that it is a Cisco router. Based on the open ports and responses to connection on those ports this router was determined to be a Cisco. You might want to elaborate here in the text if you can.

Cisco has been accused of developing "a special firewall box for the Chinese authorities which blocked the forbidden web sites on a national scale"[70].

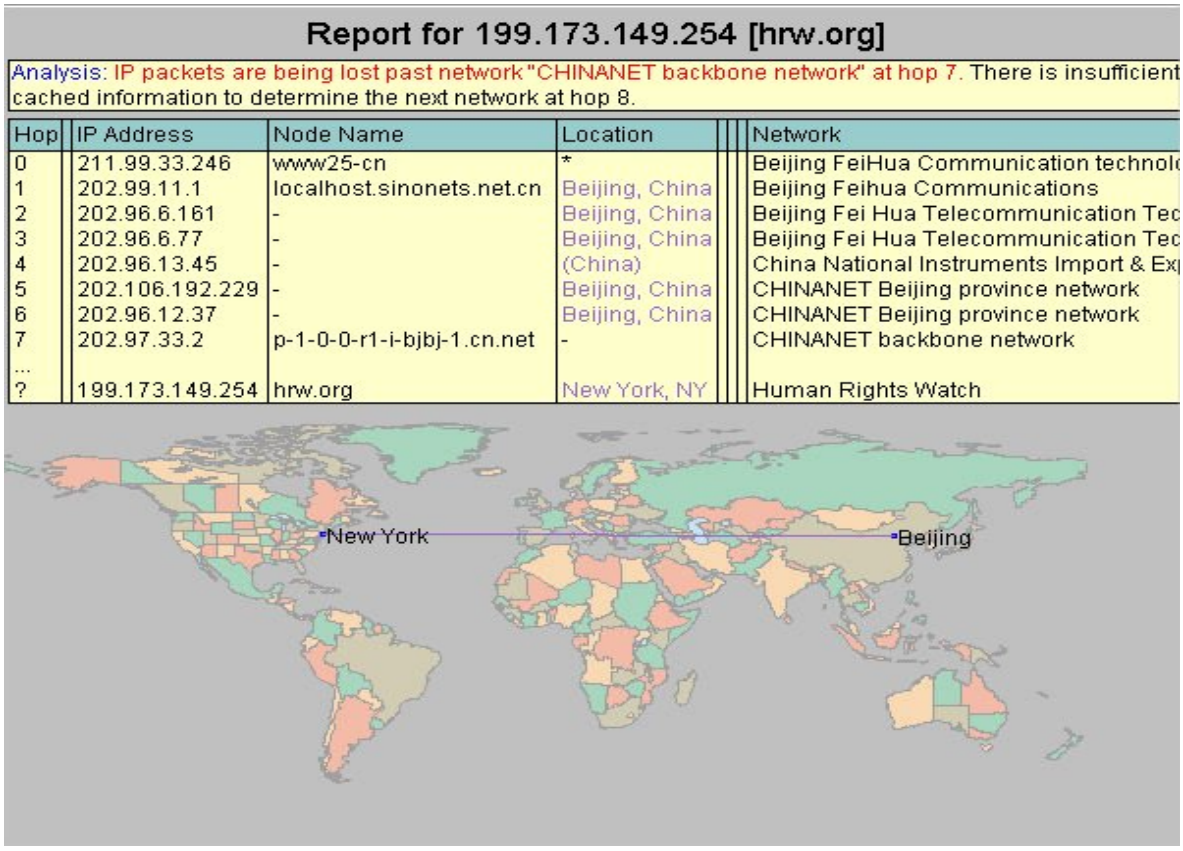


Figure 1: visual traceroute results of a request to the website of Human Rights Watch.

Round One of Project C focused on the enumeration of the user experience when trying to access controversial subject matter on the Internet. Filtering at the national backbone level is done by blocking the ip or domain name address so that users will be unable to access the content on the blocked servers. The list of blocked ip addresses/domains is secret and identification of blocked sites must be conducted through trial and error.

Instead of attempting to positively enumerate the entire list of blocked domains, this study attempted to *approximate the user experience* by using the Google search engine to retrieve lists of URL's based on different search criteria and then attempting to access each of those URL's locally and from proxy server on three backbone networks in China. In this way the study aimed to enumerate some of the blocked domains as well as approximate the user's experience in attempting to seek information on the Internet. This study shows what content is denied to a user when searching via Google and attempting to access content for specific sensitive topics in China.

[70] Tech Law Journal. News from April 16-20, 2002. Available: http://www.techlawjournal.com/home/newsbriefs/2002/04d.asp

Topic Category	Number of URLs	Google Search Terms
Falun Gong	623	"falun gong"
Human Rights	938	"human rights"
Minorities	2252	"inner mongolia" "mongolia china" "east turkestan" "uighur" "uyghur"
News	853	"news"
Anonymous Proxy	680	"Anonymous Web Proxy"
Religion	1291	"islam" "christianity" "judaism" "hinduism" "buddhism" "taoism" "shaolin"
Taiwan	712	"taiwan" "taiwan independence"
Tiananmen	751	"tiananmen"
Tibet	779	"tibet"

Total URLs Scanned: 8878
Total URLs inaccessible locally: 647
Total Live URLs: 8231

Category	URLs	Down	Total			
Falun Gong	623	57	566	ChinaGBN 144	ChinaNET 124	UniNET 113
Human Rights	938	53	885	CerNET 85	ChinaGBN 80	UniNET 73
Minorities	2251	173	2078	CerNET 565	ChinaNET 280	UniNET 286
News	853	78	775	CerNET 46	ChinaNET 53	UniNET 48
Proxy /Anon	680	43	637	ChinaGBN 52	ChinaNET 61	UniNET 70
Religion	1291	93	1198	CerNET 125	ChinaNET 134	UniNET 119
Taiwan	712	51	661	CerNET 97	ChinaNET 120	UniNET 98
Tiananmen	751	68	683	ChinaGBN 135	ChinaNET 117	UniNET 108
Tibet	779	31	748	CerNET 93	ChinaNET 95	UniNET 87

* Testing was conducted in July-August 2002. Consistent testing conditions were difficult to maintain as proxy servers would become unavailable for periods of time and new proxy servers had to be used.

CHINANET
ChinaNET is the largest Internet Service provider in China.
(www.chinanet.cn.net)

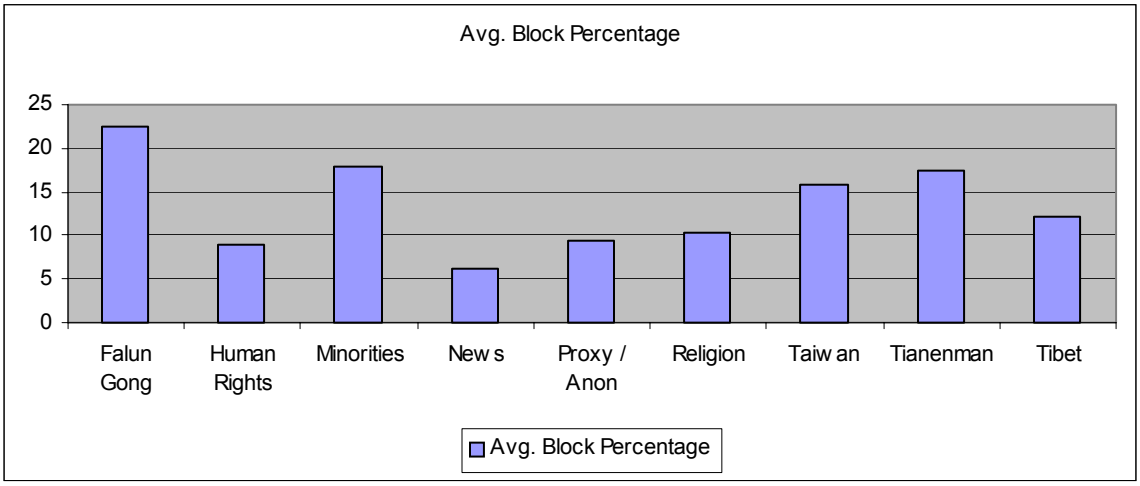
CHINAGBN
The Golden Bridge Project, developed by Jitong Communications,is a key communications network designed to serve the finance and economy sectors.
(www.gb.com.cn/english/)

CERNET
The China Education and Research Network is the first nationwide education and research computer network in China.
(www.edu.cn/HomePage/english/cernet/)

UNINET
Uninet is the first commercial Internet Service Provider in Shanghai, China and provides services foreign business, foreign consulates and the general public.
(www.uninet.com.cn)

Category	Block URL Percentage	Block URL Percentage	Block URL Percentage
Falun Gong	ChinaGBN 25.4%	ChinaNET 21.9%	UniNET 19.9%
Human Rights	CernNET 9.6%	ChinaGBN 9.0%	UniNET 8.2%
Minorities	CernNET 27.1%	ChinaNET 13.4%	UniNET 13.7%
News	CernNET 5.9%	ChinaNET 6.8%	UniNET 6.1%
Proxy/Anon	ChinaGBN 8.1%	ChinaNET 9.5%	UniNET 10.9%
Religion	CernNET 10.4%	ChinaNET 11.1%	UniNET 9.9%
Taiwan	ChinaGBN 14.6%	ChinaNET 18.1%	UniNET 14.8%
Tiananmen	ChinaGBN 19.7%	ChinaNET 17.1%	UniNET 15.8%
Tibet	CernNET 12.4%	ChinaNET 12.7%	UniNET 11.6%

Average Block Percentage



Falun Gong

Falun Gong a form of qigong which combines special exercises and meditation with Buddhist and Taoist principles. The group has been labelled a "dangerous cult" by Chinese authorities and has been outlawed. Websites supportive of Falun Gong are blocked by the PRC.

http://www.falundafa.org/
http://faluninfo.net/
http://www.fofg.org/
http://clearwisdom.net/
http://www.falungonginfo.net/

Human Rights

Human Rights organizations are extremely critical of the human rights abuses perpetrated by the PRC. The websites of Human Rights organizations are routinely blocked by the Chinese authorities.

http://www.hrw.org/
http://www.derechos.org/
http://www.hrichina.org/
http://www.amnesty.org/
http://www.liberty-human-rights.org.uk/

Minorities

Minority groups such as the Uighur population of Xinjiang (Republic of East Turkestan [1944]) and the population of Inner Mongolia face repression at the hands of PRc authorities for any nationalist or independence activism. Websites containing pro-independence information about minority groups in China are blocked.

http://www.taklamakan.org/
http://www.mongolianews.com/

http://www.innermongolia.com/
http://www.uyghuramerican.org/
http://www.uygur.org/

News

A recent study conducted by the CNNIC found that the primary information gathered online by Chinese Internet users was news (74.0%). However, the Chinese authorities sporadically block Internet access to news sources.

http://news.bbc.co.uk/
http://www.cbsnews.com/
http://www.worldnews.com/
http://www.voanews.com/
http://www.abc.net.au/news/

Proxy/Anonymity

Websites that provide web-based anonymous proxy servers or information on how to find and use publicly available proxy servers which can be used to bypass the blocking and internet surveillance mechanisms deployed by the Chinese authorities are blocked in the PRC.

http://www.silenter.com/
http://www.guardster.com/
http://www.goproxy.com/
http://www.safeproxy.org/
http://www.proxyportal.com/

Religion

The Chinese authorities see religion as a source of instability, separatism, and subversion and have increased efforts to crackdown on and control the dramatic growth of religion in the PRC. Along with persecution and imprisonment of religious activists the authorities have blocked access to religious websites.

http://www.moslem.org/
http://www.clarifyingchristianity.com/
http://www.masters-of-shaolin.com/
http://www.hinduism.net/
http://main.chinesephilosophy.net/daojia.html

Taiwan

The People's Republic of China views Taiwan as an integral part of China and is strongly opposed to Taiwan independence or separation of any form. Websites that contain information supporting the independence of Taiwan are blocked in the PRC.

http://www.president.gov.tw/
http://www.taiwanese.com/

http://home.sina.com/
http://www.chinatimes.com.tw/
http://www.taipei.org/

Tiananmen

On June 4 1989 the Chinese government ordered the military to brutally suppress a pro-democracy protestors gathered in Tiananmen Square. Troops and tanks fired on the unarmed crowd comprised mostly of students. Websites telling the story of Tiananmen are blocked in China.

http://www.tsquare.tv/
http://www.fillthesquare.org/
http://www.democracy.org.hk/
http://www.christusrex.org/
http://www.dfn.org/

Tibet

Chinese authorities heavily censor Internet content concerning Tibet. Websites that support the Dalai Lama are blocked as are websites that provide information on human rights abuses in Tibet.

http://www.tibet.com/
http://www.savetibet.org/
http://www.tibet.org/
http://www.tibet.net/
http://www.milarepa.org/