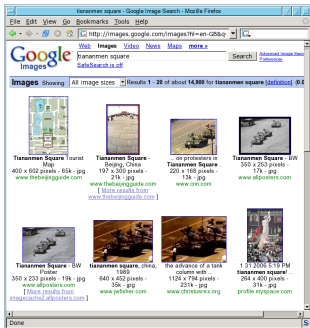


Internet censorship in China



Steven J. Murdoch

www.cl.cam.ac.uk/users/sjm217



UNIVERSITY OF
CAMBRIDGE

Computer Laboratory



OpenNet Initiative

www.opennet.net

This talk discusses the approaches to Internet censorship in China



The Internet in China



Social techniques for censorship



Technical restriction mechanisms



Examples of blocked websites

China has the second largest Internet user population and by far the largest pervasive censorship system

	Internet users (millions)	Population (millions)
United States	211	302
China	137	1 317
Japan	86	129
⋮		
Turkey	16	76
Vietnam	15	85
Australia	15	21

However, its existence is sometimes denied, or its extent downplayed

“In China, we don’t have software blocking Internet sites. Sometimes we have trouble accessing them. But that’s a different problem. . . . We do not have restriction at all.”

Chinese official at 2006 Internet Governance Forum, Athens

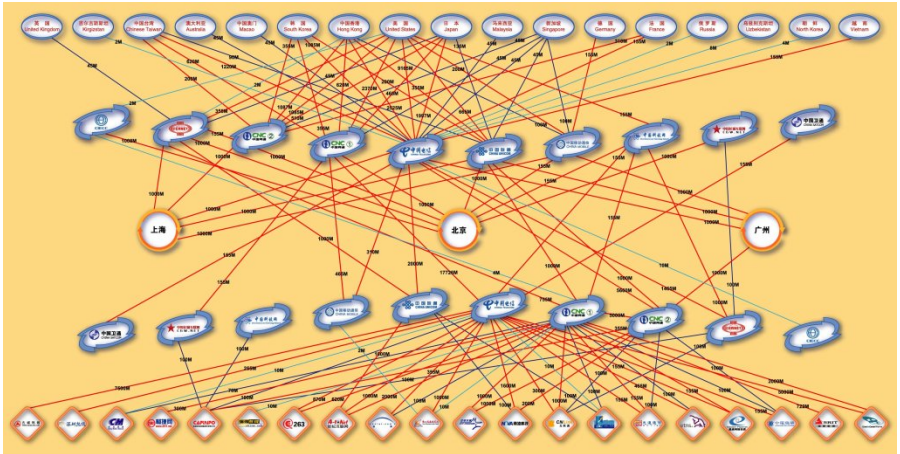
Material is blocked if it may threaten state control or social stability

- Topics targeted for blocking include:
 - Foreign news websites (including HK)
 - Human rights
 - Regional autonomy (Uyghur, Tibetan, Mongolian)
 - Software for bypassing censorship measures
- Censorship rapidly reacts to social and technological change, but has inconsistent and volatile coverage
- Sophisticated technology that underlies the “Great Firewall of China” has not been deployed by any other country (so far)

Control is exercised through interlinked social and technological means

- Technical mechanisms are blunt and easily circumvented
- Social techniques are more robust and versatile
- Selective enforcement can create a culture of fear and uncertainty without punishing many people
- Indirect control insulates government from criticism
- Complements technical measures: blocking makes it clear which material is disapproved of; social techniques encourage the population not to test these boundaries

Internet map of China (2003)



Source: CNNIC

Access providers are licensed and heavily regulated

- Ministry of Information Industry licenses the 7 Internet access providers (3 to come)
- This centralisation of control permits both blocking and surveillance (“Golden Shield”)
- Internet service providers (ISP) must monitor customer activities and keep these records for 60 days
- Internet cafés must install filtering software, copy users’ identity card and record their activities



Content providers are controlled through liability legislation

- Websites hosted in China must register with the government
- By allocating criminal and civil liability, sites are encouraged to police themselves
- Some formal guidance is given, but often operators must derive government wishes from demands for content removal
- Vague rules allow wide discretion by the authorities



Individuals are restricted by external influence and self-censorship

- ISP customers must register their identity with the police
- Well publicised surveillance activities encourage self-censorship
- In 2006, 52 people were imprisoned for online activities

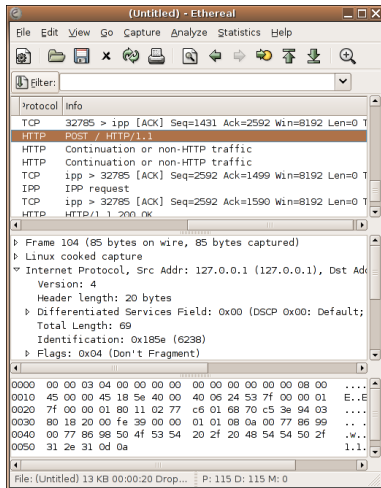
“while China is the world’s biggest jailer of journalists, China is also writing the manual on how to control your press and citizen media – and hence your national discourse – while jailing a minimum number of people.”

Rebecca MacKinnon

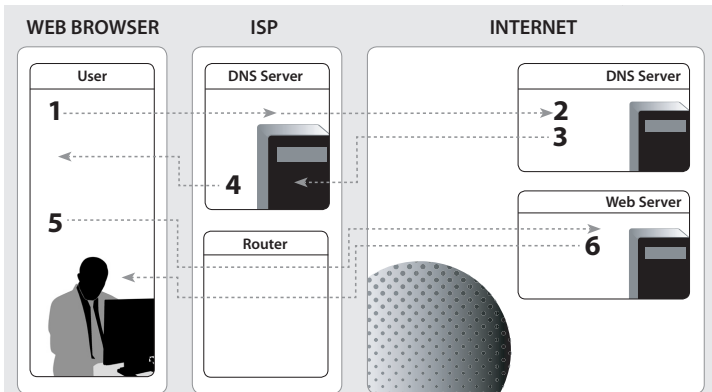


Technological filtering can be detected through Internet monitoring

- By testing Internet connections within the country, lists of blocked sites can be built
- Analysis can differentiate errors from intentional blocking
- In many cases, both the mechanism of blocking can be established, as can the location
- However, discerning the intention is more difficult
- Self-censorship is much more difficult to measure

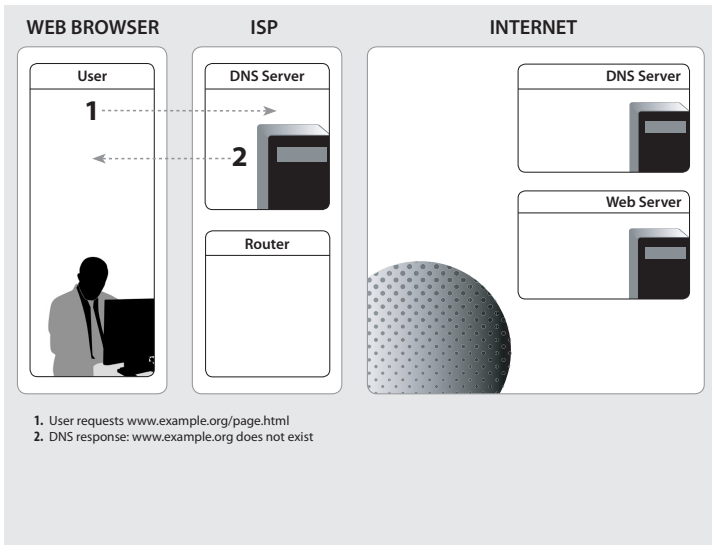


Normal web browsing

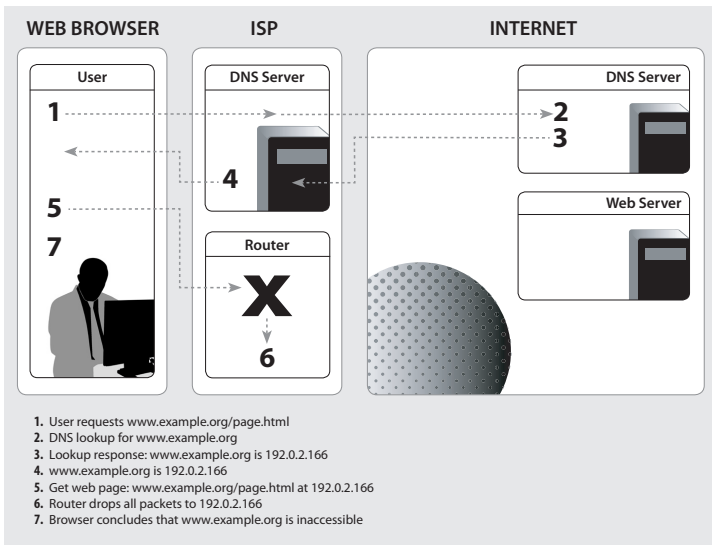


1. User requests `www.example.org/page.html`
2. DNS lookup for `www.example.org`
3. Lookup response: `www.example.org` is `192.0.2.166`
4. `www.example.org` is `192.0.2.166`
5. Get web page: `www.example.org/page.html` at `192.0.2.166`
6. Here is `www.example.org/page.html`

DNS tampering

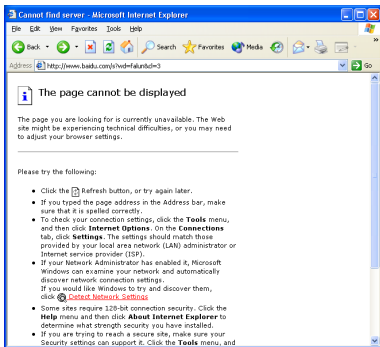


IP blocking



Certain keywords are also blocked

- Some words, both in Chinese and English, are banned regardless of website used
- When this mechanism has been triggered, the website appears to be broken
- Future requests to the same website will fail for around 20 minutes



A wide range of topics are subject to censorship, to varying extents

- News

news.bbc.co.uk

- Human rights

www.hrichina.org

- Regional autonomy

savetibet.org

- Circumvention tools

psiphon.civisec.org

- Pornography

www.playboy.com



A wide range of topics are subject to censorship, to varying extents

- News

news.bbc.co.uk

- Human rights

www.hrichina.org

- Regional autonomy

savetibet.org

- Circumvention tools

psiphon.civisec.org

- Pornography

www.playboy.com



A wide range of topics are subject to censorship, to varying extents

- News

news.bbc.co.uk

- Human rights

www.hrichina.org

- Regional autonomy

savetibet.org

- Circumvention tools

psiphon.civisec.org

- Pornography

www.playboy.com



A wide range of topics are subject to censorship, to varying extents

- News
news.bbc.co.uk
- Human rights
www.hrichina.org
- Regional autonomy
savetibet.org
- Circumvention tools
psiphon.civisec.org
- Pornography
www.playboy.com



A wide range of topics are subject to censorship, to varying extents

- News

news.bbc.co.uk

- Human rights

www.hrichina.org

- Regional autonomy

savetibet.org

- Circumvention tools

psiphon.civisec.org

- Pornography

www.playboy.com



Conclusions

- China's Internet censorship system incorporates sophisticated technical measures, and is of a previously unseen scale
- However, its strength comes from a combination of technical and social measures
- While censorship is pervasive, the list of blocked material is continually adapting to social and economic demands
- The complexity of controlling 137 million Internet users is managed by deputising the Internet community through incentives of liability and accountability

For further information on this topic

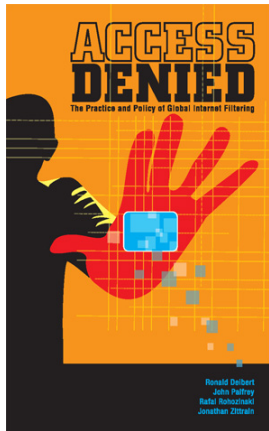
Access Denied: The Practice and Policy of Global Internet Filtering

by Ronald J. Deibert, John G. Palfrey,
Rafal Rohozinski and Jonathan Zittrain.
Published by MIT Press (November 2007)

Global Internet Filtering Conference

Oxford Internet Institute, 18 May 2007.

cyber.law.harvard.edu/oniconference07/



Acknowledgements: Thanks to Jane Gowan for the filtering graphics and to Stephanie Wang for contributing to this research