Who Controls the Past
Controls the Future

Who Controls the Present
Controls the Past

Nothing gives rest but the sincere search for truth.

-Pascal


Greetz
from Room 101
Kenneth Geers

1984

- *Nineteen Eighty-Four* (Orwell)
- Govt IW vs own populace
- Ministry of Truth, Thought Police
- Two-way telescreens
- Room 101
- Can Big Brother reprogram Winston?

2007

#The Internet is life

#Goodbye traditional media

#Unpredictable nature of the Net

#Weaponization of the Net

#Government repression &
legitimate criminal pursuit

Greetz 101 Palace Strategy

#Rule #1: Never trust the Internet

#Must shrink the info space

  #Family-centric calendar (T-stan)

  #DDoS the news (K-stan)

#Good reasons for censorship

  #Criminal, cultural, religious

  #Political adversaries

Greetz 101 Tactics

- **Goal #1:** the delivery of unaltered messages to your citizens
  - (And denial of the same to your rivals)
- The Internet can help
  - Surveillance/manipulation
  - State-owned telecoms

Cyber S.W.A.T.

- Read, delete, modify data packets
  - By IP, domain, strings, etc
- Call law enforcement when necessary
- Plausible deniability in Cyberspace
- International politics? Human rights? Buehler?

Which Internet?

- The Eastern Albonian Internet
  - Few international sites
  - Heavily regulated local sites
- Some gvts open, proud of censorship
  - Better than silence
    - Secrecy may imply impropriety

Practical Challenges

- Filtering Net traffic is not easy
  - Networks are complex, dynamic
  - Change control a nightmare
- No network is air-tight
  - Sophisticated users
  - Hostile network operations

Denial of Sin (DoS)

Sex words make great keywords

  # Pornography easier than politics

Blacklists should be double-checked by real people

  # Marinated chicken breasts

  # Middlesex County

How to poison a webserver

Programming & Politics

- Challenge for AI: words in context
  - Was that constructive criticism?
  - Humour, irony, sarcasm, satire?
- SME required
  - History, language, culture
  - Impossible in Internet era
    - Esp for one-man show: NK, T-stan

The Despot's Challenge

- Over/under-blocking
  - Blacklisting
    - String matching: “royal family” and “corrupt”
    - Should be 2-stage system
  - Whitelisting
    - Deny anything not explicitly allowed

The Human Factor

- Influence user behaviour
  - Intimidation = self-censorship
- Security personnel
  - Traditional skills inadequate
  - Recruits need skillz

The Connectivity Commandments

I. Accounts must be officially registered

II. All activity must be directly attributable to an account

III. Users may not share or sell connections

IV. Users may not encrypt communications

The Executable File

- Open source vs corporate
  - Manual conf vs point-and-click
- Hardware & software
  - .mm .by .zw .cu bought from .cn

The Corporate Connection

- Collaboration or conspiracy?
  - Target of privacy advocates
- Industry “politically neutral”
- Customization is key
  - Exotic locales, languages
  - Default categories: pornography, gambling
- How do you advertise censorship?

DansGuardian



- Free Net surveillance
- “Unobstructive” to “draconian”
- Filter by URL/IP/domain/user/ content/file/extension/POST
- PICS, MIME, RE, https, adverts, compressed HTML, algorithm
- Phrase-weighting, whitelist, stealth modes

Chance, Fate or TCP/IP?

- Router-based control
  - Blacklist IPs, etc
- DNS hijacking
  - Owning the dictionary
- Modified Mirrors
  - Altering adversary websites
- Cyber sting operations
  - Not now, Darling, we have company…

The Most Repressive Governments in Cyberspace

- The Top Ten calculus
  - Reporters Without Borders
  - OpenNet Initiative
  - Electronic Frontier Foundation
  - ITU Digital Access Index
  - Freedom House
  - Current events
  - Donuts and coffee

Freedom House



Reporters Sans Frontières

REPORTERS WITHOUT BORDERS
FOR PRESS FREEDOM

World Press Freedom Index 2006 - The rankings

1	Finland	0,50
-	Iceland	0,50
-	Ireland	0,50
-	Netherlands	0,50
5	Czech Republic	0,75
6	Estonia	
-	Norway	
8	Slovakia	
-	Switzerland	
10	Hungary	
159	Nepal	73,50
160	Ethiopia	75,00
161	Saudi Arabia	76,00
162	Iran	90,88
163	China	94,00
164	Burma	94,75
165	Cuba	95,00
166	Eritrea	97,50
167	Turkmenistan	98,50
168	North Korea	109,00





#10 Zimbabwe



Cyber Tasking

- Oct 20, 2006: Pres Mugabe to Central Intelligence Organisation (CIO)
  1. Infiltrate ISPs
  2. Monitor private communications
  3. Flush out Internet journalists
- Police as café attendants, surfers
  - Find those posting negative info
  - "…some computer training first"

Guarding the Gateway

- Monopoly sought for pro-gov Tel*One
  - All traffic, all profits
- Interception of Communications Bill
  - Signif HW/SW expenses for ISPs
  - No court challenges
  - Threatened to shut down
- Monitoring system bought from China

.zw Defacement



Ministry of Health



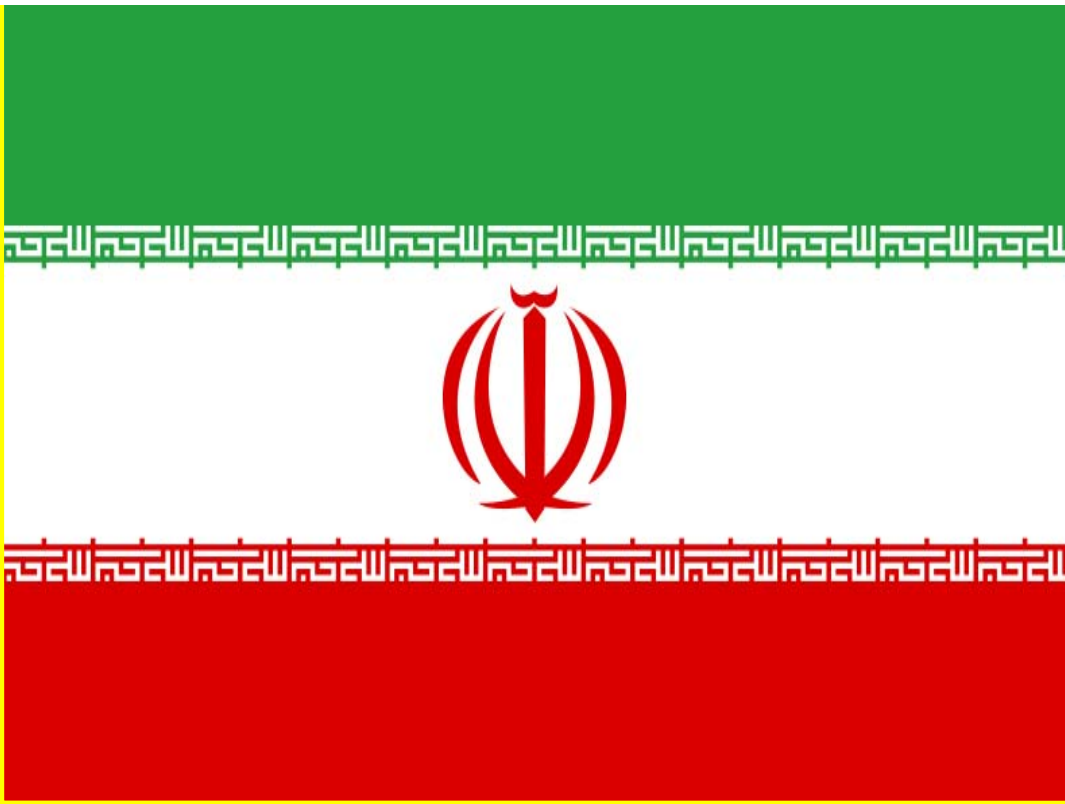


and Child Welfare

Command Tribulation Ownz your b0x

Jesus loves you





#9 Iran



Selective Surveillance

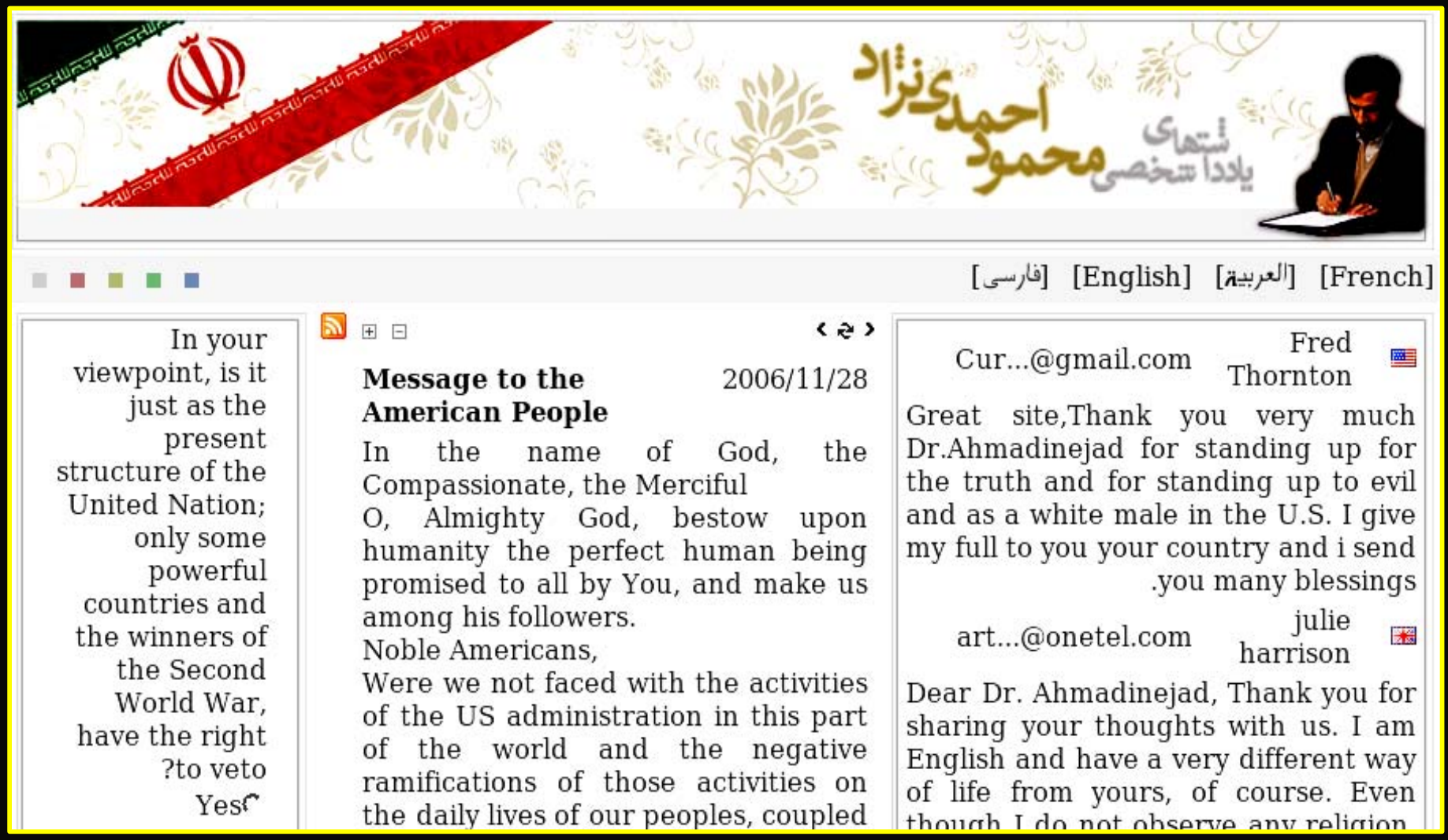
- Phenomenal growth
  - 2001 (1M), 2007 (5M), 2009 (25M)
- Mature network monitoring, but laws not routinely enforced
- Sites, not user behavior, blocked
  - Muslim values emphasized
  - ± 1/3 websites blocked: porn, anonymizers, politics
  - More likely blocked if in Farsi

A Blogger's War

- No “immoral” reporting, anon pubs
- Web still “most trusted” news
  - Forums can be openly critical
- Net savvy: Mirroring, blacklist posting, RSS
- Blogging huge, even by government
  - Accused CIA of authoring blogs
  - Death threat against IR blogger

The President's Blog

http://www.ahmadinejad.ir/



.ir Defacement







#8
Saudi Arabia



A Moral Internet

- King A.A. City for Sci & Tech
  - National-level proxy
  - Eliminate net's “negative aspects”
  - Caching, blacklisting, triage
  - Pop-ups: “disallowed”, “logged”
  - Encryption forbidden
- ISPs must conform to Muslim values, traditions, and culture

Technology vs Bureaucracy

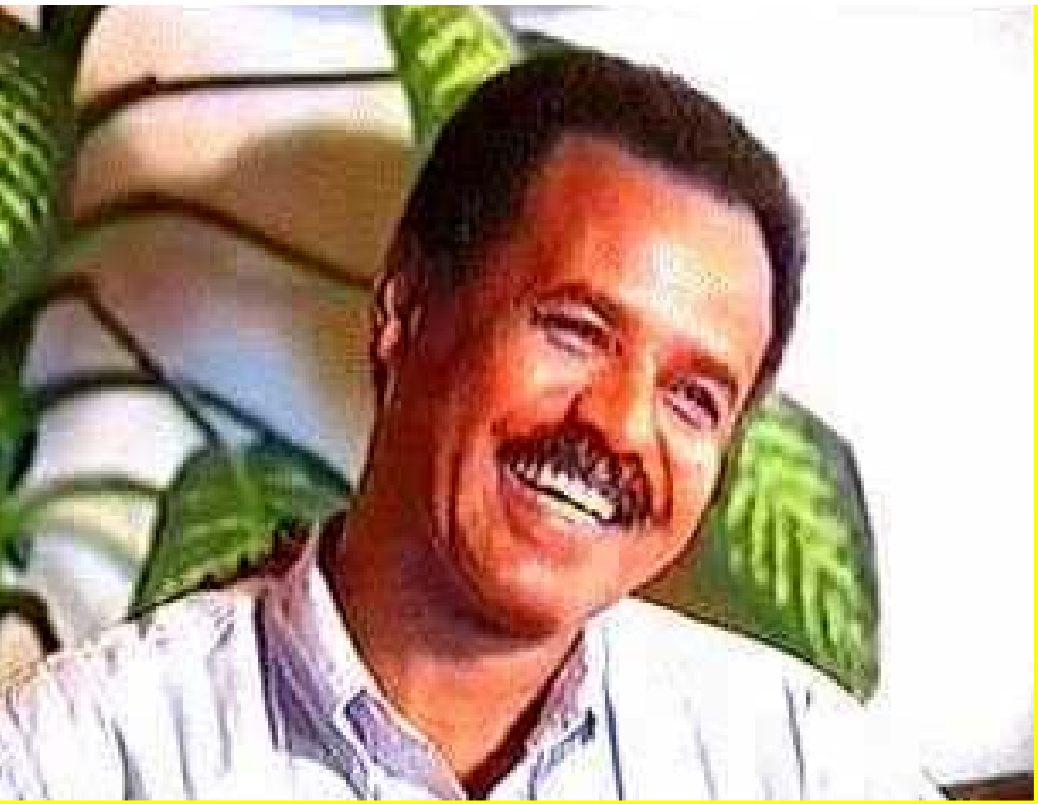
- Censor mix: morality and politics
  - Porn, “unofficial” histories
  - Blacklist removal (and add) forms
- Politically-focussed blocking
  - Cat-and-mouse game with MIRA
- SA GVT: hard to keep up
  - Highly educated citizenry
  - Direct connect to foreign ISPs

.sa Defacement



We are : Mianwalian , PakBrain ,saudia_hacker

Shoutz to : net^DeViL, PRI[ll, all staff on irc.gigachat.net





#7 Eritrea



Last Online

- Tradition of clandestine radio
  - 1 transmitter = 3 anti-ER stns
- Disinformation now online
- Telecom Service of Eritrea (TSE)
  - NOV 2000: 512 kps to 4 ISPs
  - Opposition sites init accessible
- Few wealthy enough to own computer
  - ISPs typically walk-in

First Offline

- 2001: human rights downhill
  - No reporters, no NGOs
- 2004: cyber cafes moved to “educational and research” centres
  - Pornography cited; diplomats skeptical
- Politics discussed *outside* Eritrea





#6 Belarus



Ah, The Good Old Days

- President controls print, radio, TV
- State Ctr for Info Security (GCBI)
  - Owns TLD (∴ DNS, website access)
- Beltelecom: state-owned monopoly
  - “Persecution by permit”
- Crime: defaming “dignity” of leaders
- 2001, 2003, 2004, 2005: DoS of websites critical of President
- 2006: “flash-mob” arrested

Cyber Showdown

- 3/19/2006: Election Day
  - 37 opposition/media sites down
  - Pres challenger site “dead”
  - DNS errors reported
- 3/25/2006: demonstrators arrested
  - Internet inaccessible from Minsk
- Not comprehensive, but selective
- Pres Lukashenka won by wide margin

.by Defacement









#5 Burma

Illegal: Incorrect Ideas

- Net penetration ± 0.6%
- “Myanmar Internet”, state email
  - No politics, webmail, anon, porn
- Anonymity impossible?
  - Cyber cafés: name, address, ID
  - Frequent screenshots
- **Prison:** unreg computers, shared accounts, “incorrect ideas/ opinions”, “criticism”

Resistance is Futile

- Very little room for manoeuvre
- Online activism (abroad) since 1996
- International pressure
  - Shareholder threats, business boycotts, nation-state sanctions
- Data filtering provider
  - Denied knowledge of SW sale
  - WWW: PM & Sales Dir closing deal

.mm Defacement



#4 Cuba







No Private Connections

- Highly educated, but < 2% online
  - GVT owns nearly all computers
- Cyber café: 1 hour = ½ monthly wage
- Cannot violate “moral principles”
  - Illegal connection = 5 yrs, counter-revolutionary post = 20 yrs
- Msg w/ dissident names crashed cmptr
  - Pop-up: “state security reasons”

Cyber Black Market

- Connection-code, HW trafficking
  - ±30 dollars/month
  - Students expelled
    - Video posted of officials announcing punishment
- Connections borrowed from expats
  - Police have threatened expulsion
- Journalist hunger strike

.cu Defacement



[[hacked by uykusuz001]]

WAR!!FOREVER WORLD PEACE!!...AND

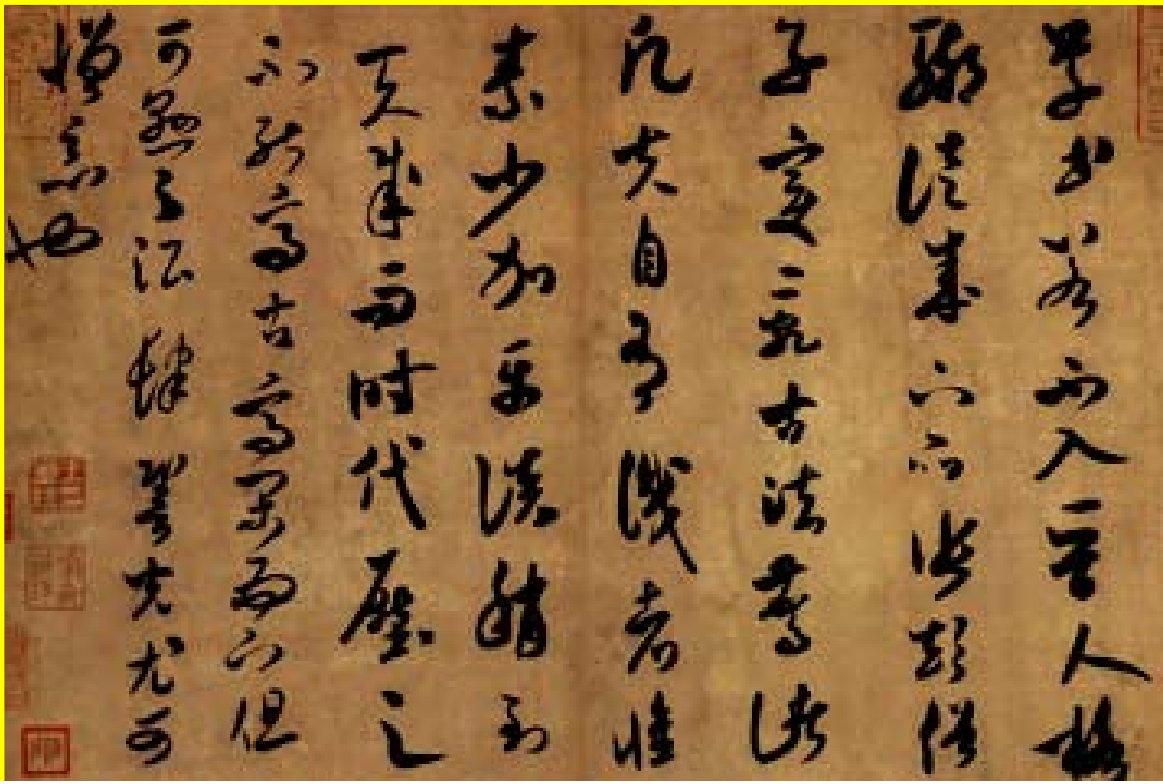
.. !! .. ONE TURK .. AGAINST THE WORLD .. !!..

...AND JUSTICE FOR ALL

#3 China







Mao on the Moon

- World's most sophisticated Net surveillance
  - Ubiquitous, mature, dynamic, precise, effective
  - Army of public/private personnel
  - Cybercafés keep logs 60 days
- Massive legal support for GVT
  - Individual privacy laws?

The Great Firewall

- **Removed:** Taiwan, Tibet, Falun Gong, Dalai Lama, Tiananmen Square
  - By keyword at national gateway
  - Missing URLs w/in TLDs
- **Edited:** blog entries
- JAN07, renewed “purification” of Net
  - “Development of socialist culture”
  - No new cyber cafes this year

.cn Defacement







#2
Turkmenistan



Father of All

- Turkmenbashi personality cult
  - All media: praise to Niyazov
- Almost NO Net access
  - None from home, no cyber cafés
  - A *few* approved websites
- 2002: 8,000 Net users (pop. 5 M)
- IT certs: 58 in 2001 (last in FSU)

“President-for-Life” Gone

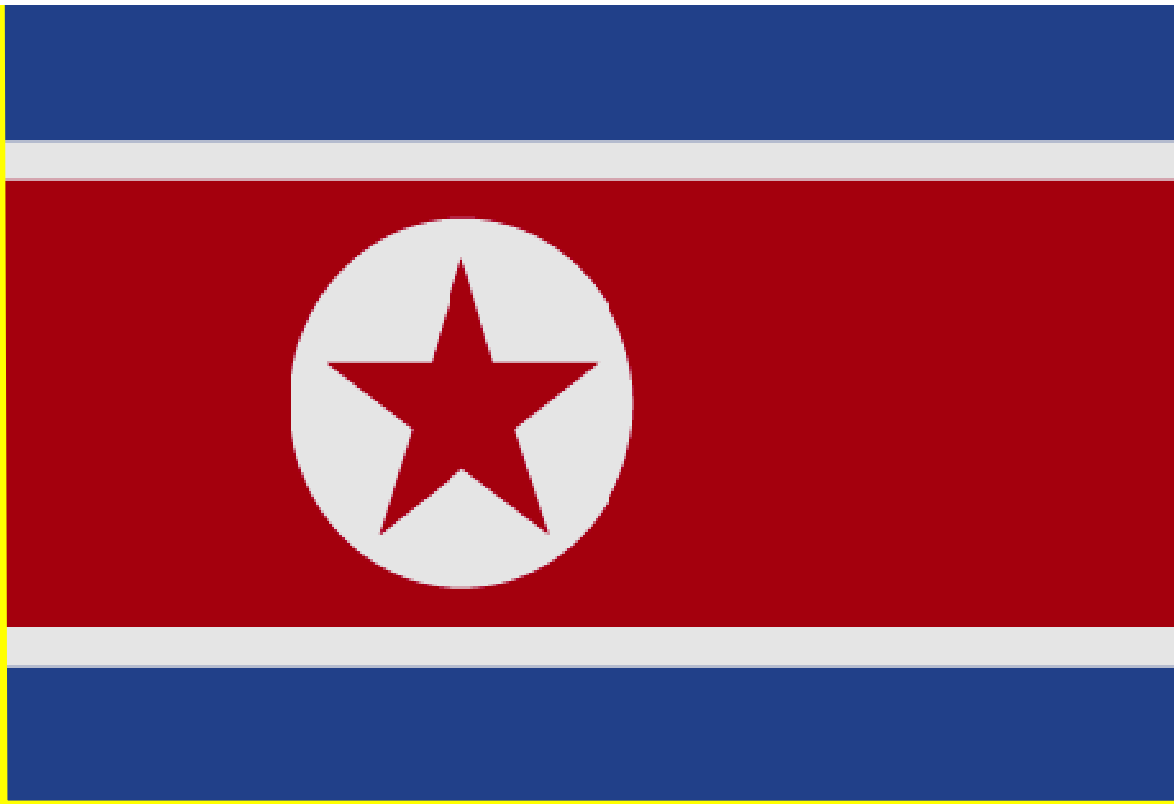
- New ruler election promise:
  - Unrestricted Internet access
- 2 cybercafés opened 2/16/2007
  - Soviet Central Telegraph bldg
  - Admin announced no censorship
  - Grand Opening: no reg required
  - But nobody showed…
- Bright side: Turkmen are gamers!

.tm Defacement



spider.tm defaced





#1
North Korea



The Real 1984

- World's most isolated country
  - Perceived Net threat extreme
- State media only, cmptrs *unavailable*
- Kim Jong-il fascinated with IT Rev
  - 2000: gave M. Albright email addr
  - Only top leaders w/ free access
- Top grads from KIS Mil Academy: elite, state-sponsored hacker unit

Greetings, Earthlings!

- K Computer Centre
  - Int'l pipe, IT hub
  - R&D, tight ACL
- Kumsong school
  - 100 male students/year
  - English, programming
  - IM, no games, no Internet
- Spain-based portal: official sites



The Future of Cyber Control

1. National security perceptions
2. Market forces
3. Big Brother helps Little Brother

China => Zimbabwe

GVT Objectives

- **Realistic goal**
  - Stop ordinary users from blatant attacks
- **Unrealistic goal**
  - Stop clever users from sophisticated attacks

Analysts Overwhelmed

- Technology faster than bureaucracy
  - SW, HW constantly evolving
  - Website content too dynamic
  - Computer network defense challenges hard to overstate

E-conomics

- Politics: power or progress?
- Monopoly hurts efficiency, vitality
- **Net thrives on information exchange**
  - Censorship slows cyberspace, economy
- Future will be ever more wired
- Fukuyama: ***The End of History***

The Future of Cyber Resistance

- Internet: champion of freedom
  - Traditional media much more susceptible to control
  - For ordinary citizens and activists
- Privacy advocates should be cautiously optimistic

Very Common Tools

- Tel/sat/web access to foreign ISPs
- Pseudonymous email
- P2P, anonymous proxies, encryption
- Dead drops, steg, covert channels
- Magic with apps/protocols/ports
- **Creativity:** text as pictures, hiding in whitespace, ?, ?



In the News

- **Psiphon:** Citizen Lab Project (UT)
- Designed for *Greetz 101* regimes
  - Free user #1 installs SW
  - Connection info sent to user #2
  - #2 crypto com to WWW via #1
- **Security is personal trust**

No Magic Bullet

- Cyberspace is anarchic
- No perfect attack
- No perfect defense
- Advice: increase vigilance at key times (elections)
- If personally targeted, very little may help you

Truth in Cyberspace

- Evidence requires:
  - Uncommon expertise
  - Infrastructure map
  - Traffic baseline
  - Multiple access points/data paths
  - Knowledge of adversary tactics
- Normally only available to BB

The Human Factor

- User sophistication rising
- Lay tech analysis possible
  - Latency, banners, errors, crashes
- Investigate outages quickly
  - General censorship or targeted?
  - Is content amenable to filtering?
- Legit or MITM … what do you think?


LIBERTY WAITS
ON YOUR FINGERS –
KEEP ON BLOGGING!
http://eff.org/bloggers/

Bibliography

"2002 Global IT IQ Report", Brainbench, March 2002, www.brainbench.com/pdf/globalitiq.pdf

"Amnesty International concerned at increasing censorship in Iran", Payvand, 12/7/06, http://www.payvand.com/news/06/dec/1067.html

Anonymous, "Cuba inches into the Internet Age", The Los Angeles Times, November 19, 2006, http://www.latimes.com/technology/la-fg-cubanet19nov19,1,2828501.story?coll=la-headlines-technology

Beer, Stan. "Iran an enemy of YouTube", Wednesday, 06 December 2006, ITWire, http://www.itwire.com.au/content/view/7795/53/

"Belarus KGB arrests U.S. Internet specialist", Reuters, October 19, 2004, http://news.zdnet.com/2100-3513_22-5417399.html

Boghrati, Niusha. "Information Crackdown", Worldpress.org, October 26, 2006, http://www.worldpress.org/Mideast/2536.cfm

"China keeps largest number of scribes in jail", Associated Press, 12/10/2006, http://www.thepeninsulaqatar.com/Display_news.asp?section=World_News&subsection=Rest+of+the+World&month=December2006&file=World_News20061210151736.xml

"A crack in the isolation of Turkmenistan: Internet cafes", USA Today (AP), 2/16/2007, http://www.usatoday.com/news/world/2007-02-16-turkmenistan_x.htm

"DansGuardian: true web content filtering for all", http://dansguardian.org

Edelman, Ben. "On a Filtered Internet, Things Are Not As They Seem", Reporters Without Borders, http://www.rsf.org/article.php3?id_article=10761

EURSOC Two. "Iran Running Scared Of The Net", 04 December, 2006,

http://eursoc.com/news/fullstory.php/aid/1260/Iran_Running_Scared_Of_The_Net.html

Fifield, Anna. "N Korea's computer hackers target South and US", Financial Times, 10/4/2004,

http://www.ft.com/cms/s/3d592eb4-15f0-11d9-b835-00000e2511c8.html

Geers, Kenneth. "Sex. Lies, and Cyberspace: Behind Saudi Arabia's National Firewall", GSEC Version 1.4, 2003,

http://www.giac.org/certified_professionals/practicals/gsec/2259.php

"The Internet and Elections: The 2006 Presidential Election in Belarus (and its implications)", OpenNet Initiative: Internet Watch, April 2006

"Internet Filtering in Burma in 2005: A Country Study", OpenNet Initiative, October 2005,

http://www.opennetinitiative.net/burma

"Internet Filtering in China 2004-2005: A Country Study", The OpenNet Initiative, April 14, 2005

"Internet Filtering in Iran in 2004-2005", OpenNet Initiative, www.opennetinitiative.net/iran

"Internet fuels rise in number of jailed journalists", Committee to Protect Journalists, Special Report 2006,

http://www.cpj.org/Briefings/2006/imprisoned_06/imprisoned_06.html

"Internet-based SMS blocked for Iran's elections", IranMania, December 04, 2006,

http://www.iranmania.com/News/ArticleView/Default.asp?NewsCode=47753&NewsKind=Current%20Affairs

"Iran blocks YouTube, Wikipedia and NYT", The Bangkok Post, Dec 6, 2006,

http://www.bangkokpost.com/breaking_news/breakingnews.php?id=114803

Karmanau, Yuras. "U.S. citizen arrested by Belarusian KGB", Associated Press, October 19, 2004, http://www.signonsandiego.com/news/world/20041019-0455-belarus-us-arrest.html

Kennicott, Philip. "With Simple Tools, Activists in Belarus Build a Movement", Washington Post, September 23, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/22/AR2005092202012_pf.html

Last, Alex. "Eritrea goes slowly online", BBC News, 14 November, 2000, http://news.bbc.co.uk/2/hi/africa/1023445.stm

Lobe, Jim. "RIGHTS GROUPS CONDEMN IRAN'S INTERNET CRACKDOWN", Eurasianet, 11/16/04, http://www.eurasianet.org/departments/civilsociety/articles/eav111604.shtml

LonghornFreeper. "North Korean military hackers unleash "cyber-terror" on South Korean computers", Free Republic, 05/27/2004, http://www.freerepublic.com/focus/f-news/1143440/posts

Magee, Zoe. "Iran's Internet Crackdown", ABC News, Dec. 6, 2006, http://abcnews.go.com/International/print?id=2704399

Manyukwe, Clemence. "Zimbabwe: Paranoia Grips Govt", OPINION, Zimbabwe Independent (Harare), November 10, 2006 http://allafrica.com/stories/200611100389.html

"Media warfare in the Horn of Africa", BBC Online Network, March 2, 1999, http://news.bbc.co.uk/2/hi/world/monitoring/280680.stm

Mite, Valentinas. "Belarus: Opposition Politicians Embrace Internet, Despite Digital Divide", Radio Free Europe/Radio Liberty (Bymedia.net), February 7, 2006, http://www.rferl.org/featuresarticle/2006/2/94d60147-0a69-4f28-86c3-728a651fb0d0.html?napage=2

"Mugabe's spies to infiltrate internet cafés", AFRICAST: Global Africa Network, SOUTHERN REGION NEWS, 12/04/06 http://news.africast.com/africastv/article.php?newsID=60327

"New Belarus Bill Restricts Online Dating", ABC News, http://abcnews.go.com/Technology/wireStory?id=1412972&CMP=OTC-RSSFeeds0312

New Software to Fight Web Censorship, The Irawaddy, Friday, December 01, 2006,

http://www.irrawaddy.org/aviewer.asp?a=6443&z=148

Nichols, Michelle. "Jailed journalists worldwide hits record", New Zealand Herald, December 8, 2006, http://www.nzherald.co.nz/section/story.cfm?c_id=2&ObjectID=10414439

"North Korea nurturing nerds", The Sydney Morning Herald, 10/21/2005,

http://www.smh.com.au/articles/2005/10/20/1129775892093.html

O'Brien, Danny. "A Code of Conduct for Internet Companies in Authoritarian Regimes", Electronic Frontier Foundation,

February 15, 2006, http://www.eff.org/deeplinks/archives/004410.php

Perkel, Colin. "Canadian software touted as answer to Internet censorship abroad", Canoe, 2006-12-01,

http://money.canoe.ca/News/Sectors/Technology/2006/11/30/2561763-cp.html

Peta, Basildon. "Brainwashing camp awaits Harare journalists", November 29, 2006, Independent Online,

http://www.iol.co.za/index.php?set_id=1&click_id=84&art_id=vn20061129022721568C138622

"Press Freedom Round-up 2006", Reporters Without Borders, 31 December 2006,

http://www.rsf.org/article.php3?id_article=20286

Rena, Ravinder. "Information Technology and Development in Africa: The Case of Eritrea", November 26, 2006,

http://www.worldpress.org/Africa/2578.cfm

Reyes, Nancy. "First they censored the letters, then the internet, and now, cellphones", November 28th, 2006,

http://www.bloggernews.net/12537

Slavin, Barbara. "Internet boom alters political process in Iran", USA TODAY, 6/12/2005,

http://www.usatoday.com/news/world/2005-06-12-iran-election-internet_x.htm

"South Korea probes North Korea's cyber-casino", TechCentral, 1/14/2004, Computer Crime Research Center, http://www.crime-research.org/news/2004/01/Mess1401.html (original: The Star Online (Malaysia), http://star-techcentral.com/tech/story.asp?file=/2004/1/14/technology/7106580&sec=technology)

Sprinkle, Timothy. "Press Freedom Group Tests Cuban Internet Surveillance", World Politics Watch, 08 Nov 2006, http://worldpoliticswatch.com/article.aspx?id=321

Thomas, Luke. "Iran Online: The mullahs can't keep their people from the world", March 02, 2004, http://www.nationalreview.com/comment/thomas200403021100.asp

"Turkmenistan", Reporters Without Borders, http://www.rsf.org/article.php3?id_article=10684

Usher, Sebastian. "Belarus protesters turn to internet", BBC, 21 March 2006, http://news.bbc.co.uk/2/low/europe/4828848.stm

Usher, Sebastian. "Belarus stifles critical media", BBC, 17 March 2006, http://news.bbc.co.uk/2/low/europe/4818050.stm

Voeux, Claire and Pain, Julien. "Going Online in Cuba - Internet under surveillance", Reporters Without Borders, October 2006, http://www.rsf.org/article.php3?id_article=19335

Zimbabwe, Amnesty International, http://www.amnesty.ca/zimbabwe/

"Zimbabwe: Revised Bill Still Threatens Rights of Access to Information And Free Expression", Media Institute of Southern Africa (Windhoek)", PRESS RELEASE, December 1, 2006, http://allafrica.com/stories/200612010376.html