Greetz from Room 101

Kenneth Geers

www.chiefofstation.com

Black Hat 2007

Contents: A Cyber War in Three Parts

Preface

1984

Have you ever embellished a resume, or lied when you told a hot date that you were in love with her? Guess what: you have engaged in Information Warfare. And governments are just like you and me … only the stakes are usually much higher.

In the novel *Nineteen Eighty-Four*, George Orwell imagined a government that waged full-time Information Warfare (hereafter IW) against its own people. There is a Ministry of Truth, which is in charge of lies. Thought Police punished something called thoughtcrime, and used technology in the form of two-way telescreens to keep an eye on everyone. Room 101, a torture chamber in the Ministry of Love, awaits the rule breakers. There, Big Brother attempts to reprogram wayward souls. Citizen Winston Smith worked in the Ministry of Truth, rewriting history in an attempt to match current government positions.

As always, truth is stranger than fiction. There are many countries on Earth where the only media available carry stories that are carefully crafted by government censors, and the government's point of view will be the right one, no matter how many times it may have changed in the past. At one point in 1984, Winston was forced to write that his country, Oceania, had *always* been at war with its there-to-fore ally, Eurasia. Life paused for a moment, as everyone absorbed the new reality, and then it quickly returned to normal.

2007

Fast-forward to DEFCON 15. The indisputable power of the Internet is growing by the day. Students, politicians, covert operatives and televangelists all agree. To military men, the Internet is also a weapon: in a soldier's parlance, it can now kill people and break things. Last but not least, privacy advocates, law enforcement, and freedom of information warriors are all working on enormously important Internet projects, even if they are doing so for quite different purposes.

In times past, the first thing a coup plotter had to do, just before dawn, was to seize the national radio station. Printing presses – since they operate so much slower than radio waves – could wait until the afternoon. The Internet has changed the rules of the power game. Anyone who owns a personal computer and a connection to the Internet has both a printing press and a radio transmitter in their own home, and the entire world is potentially their audience. In places where there has traditionally been only government-run radio and newspaper, the Internet is not only the current final frontier in the information space, but it can also represent a grave threat to the continued power of the ruling government.

Chief of Station Intelligence Report

Palace Strategy

Rule #1: Never trust the Internet. It is dynamic, chaotic, and inherently unpredictable. The people will likely use access to the Internet to try and bring your government down. At the Cyber Office, our job will be to pare the Internet down to a manageable size.

Always remember that no matter what activist groups may say, there are good reasons to filter Internet content. There is evil among us, and it must be policed. Publicly, you can cite culture, religion, and common sense. The two-edged sword here is that Law Enforcement tools can be used against both common criminals and political adversaries.

From a political point of view, the Internet is the best way to deliver political messages efficiently and directly to the people. At the same time, software tools allow us the opportunity to deny your rivals that same opportunity. To maximize our leverage, we must ensure that all telecommunications are controlled by the state. If we can do that, surveillance and even information manipulation are only a mouse click away.

One final point. Cyber attacks are extremely hard to prove. Evidence, especially for the common man, is scarce. If a reporter asks, tell them that you do not even own a computer. Other governments may occasionally ask you a question about computers, but in reality they rarely let human rights interfere with their business interests.

Cyber Office Tactics

The Internet itself is a Trojan horse. Now that it is allowed in our country, there will be surprises. Modern data-hiding techniques mean that even your official portrait, on our national homepage, could carry a secret message within it that describes the details of a planned coup d-etat, and we would not know it. Computer networks will never be air-tight. Hostile network operations are inevitable from both internal users and from the farthest corners of the planet.

If you continue to allow the Internet into this country, we are going to need better equipment and more expertise. Some of the choices we need to make for the country are the exact same choices that are faced by home computer users: do we buy shrink-wrapped software or use freeware? Do we want it highly configurable or point-and-click? Reportedly, Burma, Belarus, Zimbabwe and Cuba have all purchased Internet surveillance systems from the People's Republic of China (PRC).

Most of the traditional security skills that we have hired in the past are simply inadequate to control cyberspace. New recruits must either possess or quickly acquire cyber expertise.

The first thing we will target is unchecked network connections. Here are the new rules:

- All Internet accounts must be officially registered with state officials
- All Internet activity must be directly attributable to individual accounts
- Users may not share or sell their connections
- Users may not encrypt their communications
- We will encourage self-censorship through physical and virtual intimidation
- We will manage access to international news sites, especially in English
- We will regulate and tax local language sites to a very high degree

In 1991, I crossed the border from Tanzania to Malawi. My bags were searched, and all foreign media was confiscated. If you really want to own your information space, this type of discipline is necessary. World history must be your history, and the future must be your future.

Finally, we are in touch with several regimes that have common cyber concerns. They have signaled that they are willing to share their work with us on tactics and lessons learned.

National Security and Traffic Analysis

In theory, it is possible to read, delete, and/or modify information "packets" based on both address and content. When our network administrators discover a violation of the law, they simply call the police, and after cross-checking telecommunications records, they knock on the perpetrator's door.

The two basic information-filtering strategies you should be aware of are blacklisting and whitelisting. Blacklisting means removing from the public domain any material content that is objectively wrong, such as the words "government" and "corrupt" appearing in the same sentence. The problem with blacklisting is that someone will find a way to fool the system – wittingly or unwittingly – by writing something like "our govrment is korrupt". Therefore, whitelisting is a more attractive way to control the information flow. The premise here is that absolutely nothing is allowed, except that which has been pre-approved by the state. We can give the people just enough politics, weather, sport, and porn, and we are done.

Freedom loves pornography. In fact, there are interesting relationships here for us to exploit. Some countries believe that pornography is absolutely wrong and must be prohibited at all cost. And they are quite open about this. That gives governments like ours legitimacy in censorship. In practice, pornography is possible to censor because sex words make great computer keywords. They are conveniently marked "vulgar" in the dictionary. Our intention, however, is not to block porn per se, but to give our citizens just enough to keep them happy.

Politics are far more difficult for computers to analyze, so there is no choice for the Cyber Office but to be ruthless. The challenge for computers is completely different, as word recognition is not enough.

Artificial intelligence is not smart enough to place the words it sees into context. Computers do not understand the nuances of politics. The author's intention may have been positive feedback, constructive criticism, humor, irony, sarcasm, or satire. Most humans don't even know the difference. Political censorship requires an army of subject matter experts fluent in the local history, language, and culture. This was difficult in ancient Egypt; in the Internet era, it is impossible.

In the future, you will surely face the so-called Despot's Challenge, which refers to the problem of both over- and under-censoring citizens' lives. In general, any censorship at all usually leads to over-censorship. In censored countries, for example, citizens cannot usually find a map of Middlesex County, and they have trouble finding a recipe for marinated chicken breasts. Censored items should ideally be double-checked by real people. Unfortunately, that is not always practical. What we know for sure is that giving the people too much information is always dangerous. However, if they have too little information to work with, they may become quickly bored and restless.

The Corporate Connection

Strict government control and network packet analysis are not a match made in heaven. Traditional methods of control, such as muscles and truncheons, are of little use in cyberspace. Fortunately, there are many software companies that make products we can buy off-the-shelf: 8e6, CensorNet, Content Keeper, Cyber Patrol, Cyber Sentinel, DansGuardian, Fortinet, Internet Sheriff, K9, N2H2, Naomi, Net Nanny, SmartFilter, squidGuard, Surf Control, We-Blocker, Websense, and more. These products can be configured for either a schoolroom or a nation-state. Default filters include common vices like pornography and gambling. These companies are often the focus of privacy advocates' criticism, but from a free market standpoint, there is a logical defense: filtering software is politically neutral.

A good example of such software is the open source tool DansGuardian. It is advertised as sophisticated, free Internet surveillance, and "a cleaner, safer, place for you and your children". Its settings can be configured from "unobstructive" to "draconian". With this software, the Cyber Office can filter by technical specifications such as URL, IP, domain, user, content, file extension, and POST. Advanced features include PICS labeling, MIME type, regular expressions, https, adverts, compressed HTML, intelligent algorithm matches for phrases in mixed HTML/whitespace, and phrase-weighting, which is intended to reduce over- and under-blocking. Furthermore, there is a whitelist mode, and stealth mode, where access is granted to the user but an alert is nonetheless sent to administrators.

Outlook

The Internet itself is a Trojan horse that we cannot trust. The Cyber Office's primary goals will be to have visibility on all network traffic within the country, and to ensure that all political messages come only from you. At the same time, we will deny your adversaries the same opportunities. All citizens will have an Internet address that can be associated with them personally. Because we own all national telecommunications, we therefore own the entire infrastructure, and can decide precisely who sees what information.

And censoring the Internet is only the beginning. In the future, it will even be possible to manipulate the so-called "truth" in cyberspace. We intend to copy the websites of our adversaries, change the information they contain, and repost them in our country. And we can run cyber sting operations that are designed solely to bring cockroaches out of the woodwork. The average user knows very little about these matters, and he will either have to trust the information he sees, or not to trust it. Either way, we win.

Exodus Non-Governmental Organization Survey

The Most Repressive Governments in Cyberspace

This Top Ten list has been compiled using information and analysis provided by, among others, Reporters Without Borders (www.rsf.org/), the OpenNet Initiative (opennet.net/), Freedom House (www.freedomhouse.org/), Electronic Frontier Foundation (www.eff.org/), ITU Digital Access Index (www.itu.int), Central Intelligence Agency (www.cia.gov), and subjective analysis of current events. By way of example, the RSF website states that the "[a]ssessment of the situation in each country (good, middling, difficult, serious) is based on murders, imprisonment or harassment of cyber-dissidents or journalists, censorship of news sites, existence of independent news sites, existence of independent ISPs and deliberately high connection charges." The evaluation of human rights and/or Big Brother-style cyber surveillance across the planet will be a never-ending task. Further, the well of ignorance and misunderstanding will always be too deep for this to be a conclusive report. Therefore, we are constantly on the lookout for corrections to errors in both fact and judgment. That said, here are the current *Exodus* Top Ten:

10 Zimbabwe

Telecommunications in Zim were among the best in Africa, but like everything else in the country – as the government desperately clings to power – have gone downhill precipitously. Internet connection is available in Harare and is planned for all major towns and for some of the smaller ones. There are two international digital gateway exchanges, in Harare and in Gweru.

One of the primary government strategies appears to try to own the gateways leading into and out of the country. The government has purchased an Internet monitoring system from China, and is working toward a monopoly solution for the state-owned Tel*One telecoms firm. The goal here is two-fold: to force all communications through one pipe, for the sake of total visibility on internal and external traffic, and to increase the cash flow into quasi-government coffers.

Legislation, including the Interception of Communications Bill (ICB), forces ISPs, some of which have threatened to shut down in protest, to spend their Zim dollars on hardware and software to support the government's monitoring programs. In country, there are no court challenges to government intercepts allowed.

In October, 2006, it was reported that President Robert Mugabe's Central Intelligence Organisation (CIO) met with the purpose of infiltrating Zim Internet service providers (ISP), in order to "flush out" journalists who were using the Internet to feed "negative information" about the government to international media. According to the report, police were informed that they should to pose as cyber café attendants and Web surfers. However, they were also told that it would be necessary for them to undergo "some computer training" first.

A police spokesman announced that the government would do "all it can" to prevent citizens from writing "falsehoods against the government." Jail terms for such offenses are up to 20 years in length.

09 Iran

Life on the Iranian Net is already vibrant, and growing at a dizzying speed. There were 1M Internet users in 2001, 10M today, and there could be 25M in 2009. The expansion has been phenomenal, especially regarding the posting of Farsi-language material online. Cybercafés and the use of broadband are rising sharply.

While Internet surveillance in Iran is reported to be among the most sophisticated in the world, the country's political culture is also the most advanced in our Top Ten list, and many of the strict rules regarding Internet usage do not appear to be routinely enforced. Cybercafé monitoring is reported to be only the occasional inspector, and while journalists are required to be free of "moral corruption" – and anonymous publications of any sort are officially prohibited – some news media are openly critical of the government, and the Web is the "most trusted" news source.

Former president Ali Mohammad Khatami stated in an interview that the Iranian government tries to have the "minimum necessary" control over the Internet. He explained that while Muslim values would be emphasized within Iranian network space, only sites that are "truly insulting" towards religious values would be censored. He argued that political sites which oppose official Iranian government viewpoints were available to the public.

According to the OpenNet Initiative, however, about one-third of all websites are blocked by the Iranian government. Among the frequently blocked sites were politics (Voice of America www.voanews.com), pornography, translation, blogging (www.movabletype.org), and anonymizing software. Similar content is more likely to be blocked if in Farsi. Commercial software known to have been used in Iran is SmartFilter by Secure Computing.

Furthermore, it is technically illegal to access "non-Islamic" Internet sites, and such offenses can elicit severe punishments. Media receive a list of banned subjects each week, ISPs must install mechanisms to filter Web and e-mail content, and there is a dedicated press court. Iranian publications are not to conflict with government goals. Since 2000, 110 news outlets are reported to have been closed, and over 40 journalists detained.

While it has been reported that Iran has engaged in widespread censorship, it has also been alleged that the government is attempting to control user behavior to a far lesser degree. In fact, Iranian Internet users are Net savvy. Since the year 2000, Iranian citizens have participated in a remarkable amount of mainstream and alternative blogging. Even President Mahmud Ahmadinejad's has one: http://www.ahmadinejad.ir/. On the downside, at least one death threat was lodged against blogger Hoder (Hossein Derakhshan), and hard-line newspaper Kayhan

accused the CIA of using Iranian blogs to undermine Iranian government.

On the bright side, there is significant movement inside the country limit the power of the government in cyberspace. In August 2004, a number of reformist news sites were blocked, but the content was quickly mirrored on other domains. In other case, an anonymous system administrator posted an alleged official blacklist of banned sites. Even some reformist Iranian legislators have openly complained about censorship, even online. One current trend among the population is a rise in Real Simple Syndication (RSS) to evade blocking.

08 Saudi Arabia

The telecommunications system in Saudi is first-rate, encompassing extensive microwave radio relay, coaxial cable, and submarine fiber-optic cable systems. Like Iran, Saudi Arabia boasts a highly educated citizenry; they have been surfing the Internet since 1994.

Government authorities in Riyadh have articulated that they seek to create a "moral" Internet through the elimination of its "negative" aspects. The primary strategy has been to require ISPs to conform to Muslim values, traditions, and culture in order to obtain an operating license. Upstream, the King Abdul-Aziz City for Science and Technology (KACST) represents a single, centralized international connection from Saudi Arabia to the outside world. KACST is a national-level proxy server uses a complicated system of cached sites, banned URLs and cyber-triage to keep an eye on inbound and outbound traffic. Encryption is forbidden. Still, Saudi officials have admitted that in the race between technology and bureaucracy, they struggle to keep up. Citizens commonly use international telephone and satellite access to foreign ISPs.

To the Saudi Web surfer, censorship appears in the form of a pop-up window, warning that the content they seek has been disallowed (in Arabic and in English) and that their request for said information was logged by government servers (in Arabic only). Officials insist that they are reasonable when it comes to blocking Internet sites. Included in the range of information that OpenNet Initiative researchers have seen withheld are religion, health, education, humor, entertainment, general reference works, computer hacking, and political activism. In Saudi Arabia, pornography is the first thing to go. Officials contend that "all" major porn sites are identified and blocked.

However, there is evidence that censorship is based on a strong mix of morality and politics. As in the book 1984, "unofficial" histories of the Saudi Arabia are banned. Officially, political sites are not supposed to be blocked, but a well-known cat-and-mouse game between Riyadh and an anti-government group called (MIRA) tells otherwise. Initially, the government tried to block the site by IP. The site's owners were forced into marathon contest of hide-and-seek via IP hopping and port randomization, while sending constantly changing addresses to its patrons by email. The challenge was to make its readership aware of the new Web location before the authorities could find it. On average, MIRA was able to stay ahead of the government for about a week at a time.

Web application logins reportedly made it more difficult for the government to see where its citizens were going. Evidently, officials decided that the effort was too much work, and finally give up.

In a Web filtering system like this, which uses a primitive type of Artificial Intelligence (AI) to evaluate Internet sites it has never seen before, the total number or percentage of banned sites and information cannot easily be known, but easily runs into the millions. At its most basic level, keywords are used to recognize and block certain types of information. In order to prevent unnecessary over-blocking, one of the unique aspects of the Saudi system is that citizens can fill out a Blacklist Removal form (there are also Blacklist Addition forms). Thus, if an individual thinks that certain information is being withheld from them in error, they have an efficient appeals process. KACST management claim that they receive over 500 forms every day.

07 Eritrea

Oral traditions in Africa are still strong, have a historical resonance, and are widely used to foster national solidarity. Radio and clandestine radio stations in the Horn of Africa play a vital role in both government and anti-government forces. Recently, one sole Sudanese transmitter offered service to three separate anti-Eritrean radio stations.

Political battles in the Eritrea are now shifting from the radio spectrum to cyberspace. Local factions, as they appeal to the hearts, minds, wallets of their supporters, are able to reach both regional and international audiences via the Internet. Sites such as Pan-African News (www.africanews.org) and Eritrea Online (www.primenet.com/ephrem) feature images from the frontlines, analysis, and everyone from African leaders to humanitarian groups making daily statements in support of their causes.

In November 2000, Eritrea became the last African country to go online. Four ISPs shared one national pipe and 512 kilobits per second. By 2005, the number of Internet users had grown to a reported 70,000. However, since few Eritreans are wealthy enough to own a computer, ISPs typically offer walk-in use. Initially, the national Telecommunications Service of Eritrea (TSE) announced that Internet access in the country would be unimpeded, and opposition and Ethiopian websites were accessible.

Since 2001, however, human rights in Eritrea have steadily gone downhill. There are no foreign correspondents in the country, and prison inmates have been confined to cells consisting of cargo containers. No International Committee of the Red Cross (ICRC) visits have been allowed. In 2004, all cyber cafes, previously only under government “supervision”, were physically transferred to “educational and research” centers. The reason given was “pornography”, but international diplomats were highly skeptical of the move.

Since that time, some ruling party members decided to post an announcement of a new political

party to the Web, but the posting was made from outside Eritrea.

06 Belarus

Life in Minsk has not changed much since the Cold War. The Presidential Administration directly controls all information flowing through the printing press, radio, television, and now cyberspace. Independent stations typically avoid news programming altogether, and even Russian TV is heavily censored.

The Beltelecom state-owned monopoly is the sole provider of telephone and Internet connectivity, although about 30 ISPs connect *through* Beltelecom. The only reported independent link is through the academic network BasNet. Beltelecom has been accused of "persecution by permit" and of requiring a demonstration of political loyalty for its services. At least one Belarusian journalist is alleged to have "disappeared". Strict government controls are enforced on all telecommunications technologies. For example, transceiver satellite antennas and IP telephony are both prohibited.
As in Zimbabwe, the Beltelecom monopoly status is intended not only for government oversight, but also for monetary gain. It is the primary source of revenue for the Ministry of Communications (MIC).

The State Center for Information Security (GCBI), in charge of domestic signals intelligence (SIGINT), controls the .by Top Level Domain (TLD), and thus manages both DNS and website access in general. Formerly part of the Belarusian KGB, GCBI also reports directly to the President. Department "K" (for Cyber), within the Ministry of Interior, has the lead in pursuing cyber crime. Internet surveillance mechanisms were reportedly bought from China. A common media crime in Belarus is defaming the "honor and dignity" of state officials.

Belarus has a long history of Internet-based political battles to examine. In each of the following years, 2001, 2003, 2004, and 2005, Internet access problems were experienced by websites critical of the Belarusian president, state referenda, and elections. According to the government, the problems were due simply to access overload, but the opposition claimed that *no one* was able to get to the sites. One of the affected sites was characterized by the Ministry of Foreign Affairs as "political pornography".

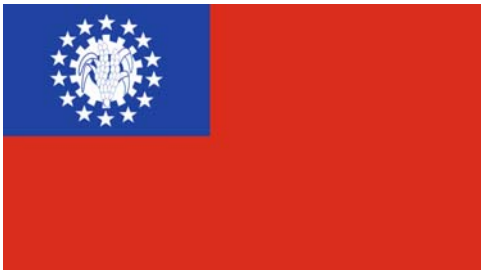
The most significant cyber showdown took place during the March 2006 Belarusian presidential elections. The opposition specifically tried to use its youth and computer savvy to organize in cyberspace. The sitting government attempted the same, but because it supporters primarily consisted of the rural and elderly its efforts were uphill at best.

Election day provided the world a case study in modern-day cyber politics. As Belarusians went to the polls, up to 37 opposition media websites were inaccessible from Beltelecom. "Odd" DNS errors were reported, and the presidential challenger's website was diagnosed as clinically

"dead". One week after President Lukashenka won the election by a wide margin, as anti-government demonstrators clashed with riot police, the Internet was inaccessible from Minsk telephone numbers. One month later, when an opposition "flash-mob" was organized over Internet, attendees were promptly arrested by waiting policemen.

The history of political cyber warfare in Belarus demonstrates that Internet filtering and government surveillance there may not be always be comprehensive, but can be highly focused on specific adversaries and at critical points in time.

05 Burma



Out of a population of XXXX, the number of Internet hosts in Burma is 42, and the number of Internet users is 78,000 (about 0.6%). For the citizen who is lucky enough to obtain Internet access, he or she travels not on the World Wide Web but instead to the "Myanmar Internet", which is composed only of a small number of officially sanctioned business websites. The two ISPs are the state Ministry of Post and Telecommunications (MPT), and a semi-private firm called Bagan Cybertech (BC). Foreign companies and embassies are allowed to have their own connections. A few cyber cafés exist, but because they require name, identification number, address, and frequent screenshots of user activity, online anonymity is virtually unattainable. Webmail, politics (i.e. Aung San Suu Kyi), anonymizers and pornography are all blocked. Only state-sponsored e-mail accounts are allowed.

According to the 1996 Computer Science Development Law, all network-ready computers must be registered with MPT. Failure to register a computer and/or sharing an Internet connection can earn Burmese citizens up to 15 years in prison. Burma's State Peace and Development Council (SPDC) prohibits "any criticism of a non-constructive type", "writings related to politics", "anything detrimental to the ideology of the state", and "writings directly or indirectly detrimental to the current policies and secret security affairs of the government". Indeed, according to Burmese law, it is fundamentally illegal to have "incorrect ideas".

Even after all that, surveys suggest that cost is still the worst part of Internet access. In Burma, the average annual income is $225. A broadband connection costs $1,300. The most common form of Internet access – dial-up – costs $6 for about 10 hours. Outside Rangoon and Mandalay, long distance fees are required. Entrance to a cyber cafe is $1.50.

There is very little resistance to Burma's Internet governance. On the international front, Web-based activist groups such as the Free Burma Coalition and BurmaNet have been organizing on-line since 1996. The data filtering company that sold its software to Burma was not keen on public knowledge of the sale. It was reported that after the company denied any knowledge of it, a privacy group found a picture on the Web of the Burmese Prime Minister and the company's Sales Director, closing the deal.

04 Cuba

Cuba boasts a highly educated population, but unfortunately less than 2% of its citizens are currently able to connect to the Internet. Without special authorization, private citizens are prohibited from buying computers or accessing the Internet. The Government owns nearly all computers on the island. Even telephone line density is less than 10 per 100 inhabitants, and wireless access remains restricted to foreigners and regime elites.

Cuban Decree-Law 209, written in June, 1996, states that "access from the Republic of Cuba to the Global Computer Network" will not violate "moral principles" or "jeopardise national security". Illegal connections to the Web can earn a prison sentence of 5 years; posting a counter-revolutionary article, 20 years. At least two dozen journalists are now serving up to 27 years in prison. It is reported that, as in several other countries in the *Exodus* Top Ten, Internet filtering and surveillance equipment were bought from China.

A human rights activist, while in Cuba, sent a test email message that contained the names of multiple Cuban dissidents. A pop-up window announced: "This programme will close down in a few seconds for state security reasons", and then her computer crashed. Further, the government's Internet monitoring program appears to be able to target specific audiences. At the Non-Aligned Movement summit in Havana (Sept 2006), conference attendees reported having no problem accessing a wide variety of websites.

There are reportedly a "few" *Correos de Cuba*, or state-run Internet cafés. The cost for 1 hour of access is $4.50, or about ½ the average monthly wage of $10. Use of a state-run email account is $1.50 per hour. As a cheaper method of access, Cubans have borrowed Internet connections from expatriates, some of whom have been summoned by the Cuban police and subsequently threatened with expulsion from the country.

In Cuba, Internet connection codes obtained from the government are used to access the Internet at certain times of the day. These codes are now bought and sold on a healthy cyber black market. For Cubans desperate for information from the outside world, these codes can fetch extraordinary sums for the impoverished country, up to a dollar a day. It was reported that students have been expelled from school for selling their codes to others, as well as for creating illicit chat forums. Following the incident, there was a video posted to the Web that showed university officials announcing their punishment to a school auditorium. Since buying computer equipment in Cuba without government authorization is illegal, there is also a black market for computer parts, and prices are said to be "extremely" high.

03 China

The People's Republic of China (PRC) possesses the world's most sophisticated Internet surveillance system. It is variously described as ubiquitous, mature, dynamic, precise, and effective. Beijing employs an army of public and private cyber security personnel, has a massive legal support system behind it, and can rely on numerous layers of policy and technical control mechanisms in order to keep a close eye on its population. However, due to a relatively freer economic system than some other countries in this list, the Middle Kingdom only registers on the *Exodus* Cyber Top Ten at #3.

While comprehensive laws support government control of traditional media and the Internet, individual privacy statutes are unclear, in short supply, and perhaps even inapplicable in terms of the information space. However, it must be said that in Asia, it is generally accepted that there is less privacy in one's daily life, and the general populace is more comfortable with government oversight than in the West.

The PRC not only has strict controls on access to the World Wide Web, but there are policemen stationed at cyber cafes, and there is a Chinese "Great Firewall" designed specifically to prevent the free flow of information into and out of the country, including, for example, the passing of videos of Chinese prison and factory conditions to human rights groups abroad. By way of example, cybercafés are one of the primary ways that Chinese citizens to access the Internet; the cafes are required to track their patrons' usage for 60 days.

The "Great Firewall" of China has been credited with providing the country with highly sophisticated censorship. Among the types of information known to be blocked are in politics, religion, and pornography. Activist testing revealed that search results came up short on Taiwan, Tibet, Falun Gong, Dalai Lama, and Tiananmen Square. In the past, Google and the BBC have both been blocked wholesale. Interestingly, sites that are often accessible are major American media sites, human rights groups' pages, and anonymizers. It is believed that search results are blocked by keyword at national gateway, and not by Chinese search engines themselves.

Western companies, for their part, have been accused of too much cooperation with the government in Beijing on cyber control issues. Google, Yahoo, and Microsoft have all collaborated with the Communist government in prosecutions. At least one U.S. congressman has termed such cooperation "sickening and evil", and compared it to the work IBM did for the Nazi government during World War II.

China is now on the cutting edge of world research and development on Internet technologies. *Exodus* worries, however, that Beijing's emphasis many these – to include IPv6 – is primarily as a strategy for population control. PRC Internet Society chairwoman Hu Qiheng has stated flatly that static China's goal is for the Chinese Internet to achieve a state of "no anonymity".

The level of sophistication in Chinese Internet surveillance can be seen by the fact that some URLs were reportedly blocked even while their corresponding top level domains (TLD) were

accessible, even when webpage content appeared consistent across the domain. In other words, the system is likely not being run solely by machines, but by human personnel as well. Further, it was reported that blog entries have not only been denied, but some of them may even have been edited, and reposted to the Web!

In March, 2007, China announced that its Great Firewall had been insufficient to keep out the Mongol invaders from cyberspace. President Hu Jintao called for a "purification" of the Internet, and indicated that Beijing would seek to tighten its control over computer networks. According to Hu, new technologies such as blogging and webcasting have allowed Chinese citizens to escape government censorship. Among the cited detrimental effects of the evasion are the "development of socialist culture", the "security of information", and the "stability of the state". Among the forthcoming initiatives was an announcement that no new cyber cafes would open in China this year.

02 Turkmenistan

President-for-Life Saparmurat Niyazov – the *Turkmenbashi*, or the Father of All – recently and unexpectedly passed away. While the country is now in a hopeful state of transition, the personality cult that Niyazov left behind has Turkmen citizens in a deep hole from which it may be difficult to escape. There is no independent press, and until recently everything written for television, newspaper, and radio was some type of hymn or tribute to Niyazov.

Telecommunications in Turkmenistan remains woefully underdeveloped. The Turkmentelekom monopoly has allowed almost no Internet access into the country whatsoever. No connections from home, and no cyber cafés. Foreign embassies and non-governmental organizations have their own access to the Internet. While they have in the past offered access to ordinary Turkmen, to take advantage of that offer was too dangerous for the average citizen. There exist only a handful of approved websites to a few Turkmen organizations. In 2001, a count of IT-qualified certifications in the former Soviet Union placed Turkmenistan dead last, with only fifty-eight in total.

In 2005, CIA reported that there were only 36,000 Internet users, out of a population of 5 million. In 2006, a Turkmen journalist who had dared to work with Radio Free Europe died quickly in prison, only three months after being jailed. Despite repeated European Union (EU) demands, there has been no investigation into the incident.

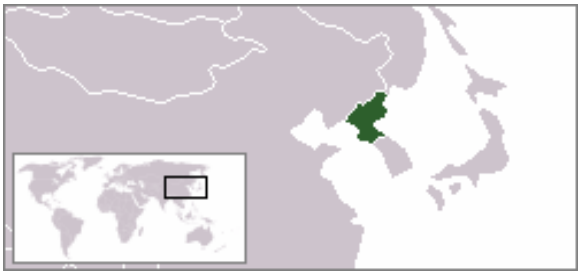
Following the demise of the Turkmenbashi, elections were held in February, 2007. Gurbanguli Berdymukhamedov won a tightly controlled vote, unmonitored by international observers. One of his campaign promises was that there would be unrestricted access to the Internet.

Days after the new leader was sworn in, 2 cybercafés opened in Ashgabat. Each is equipped with 5 computers, 5 desks, and 5 chairs. One is in the Soviet-style Central Telegraph building, the other in a run-down telephone exchange. The cafe administrator, Jenet Khudaikulieva, told a

visiting AP journalist at the Grand Opening that censorship in Turkmenistan was over. The journalist had no problem viewing international news sites, including those belonging to Turkmen political opposition groups. He reported no registration counter and no "visible" oversight. However, the price per hour, $4, is a lot to pay in a country where the average monthly income is less than $100. Indeed, almost no one attended the Grand Opening ceremony.

Life will hopefully take a turn for the better in Turkmenistan. On the bright side, reports suggest that even though connections to the Internet have been few and far between, computer gaming appears quite popular. Lastly, the use of satellite TV is on the rise, which could also be used to improve Internet connectivity.

01 North Korea



The closest thing on Earth to George Orwell's 1984 is the Democratic People's Republic of Korea (DPRK). NASA currently has better connectivity with Mars than the rest of planet Earth has with North Korea, the world's most isolated and repressed country.

Citizens are taught, however, that North Korea is superior to all other countries; therefore, the perceived threat to the nation-state from unrestricted access to the Internet is extraordinarily high. Traditional media, including both television and radio, consist of state channels only. Reminiscent of the life of Winston Smith, the DPRK has a "national intercom" cable/radio station wired throughout the country. It is a significant source of information for the average North Korean citizen, offering both news and commentary, and like the two-way telescreens of 1984 is wired into residences and workplaces throughout the country.

Computers are unavailable in the DPRK. Even if there were, the price would certainly be out of reach in a country where wild animals – and even tree bark – are scare because the citizens are so poor and hungry.

Still, Kim Jong-il, Dear Leader of the DPRK, is reported to be fascinated with the IT revolution. In 2000, he gave the visiting U.S. Secretary of State Madeleine Albright his personal email address. Still, it is currently thought that only a small circle of North Korean leadership would have unfiltered Internet access.

North Korea does have an IT school. Every year, one hundred male students, who matriculate as young as 8 years old, are chosen to attend the Kumsong computer school, where they study computer programming and English. They are not permitted to play games, or to access the Internet, but they are allowed to Instant Message each other within the school. A visiting Western journalist reported the use of Taiwanese hardware and Microsoft software.

According to the South Korean Chief of Military Intelligence, top graduates from the Kim Il-

Sung Military Academy have been chosen for an elite, state-sponsored hacker unit. Allegedly, they have been instructed to develop "cyber-terror" military options on direct orders from Kim Jong-Il. Broadly speaking, DRPK intelligence collection is said to be fairly sophisticated, with a clear collection focus on South Korea, the U.S., and Japan.

Internet connections from North Korea back to Earth are channeled via Moscow and Beijing through the Korea Computer Centre (KCC), established in 1990. The KCC provides the government in Pyongyang with its international pipe, and serves as its IT hub. Reports suggest that it downloads an officially approved, limited amount of research and development information, and pushes it to a very short list of clients.

The government's official stance on Internet connectivity is that it cannot tolerate an influx of "spiritual pollution" into the country. However, the DRPK has been caught operating a state-run "cyber casino" on a South Korean IP address. Since that discovery, South Korean companies have been under orders not to register North Korean sites without government approval.

Notes from the Underground

Cyber Control

Technology moves far faster than any government bureaucracy. The Internet changes every second. We post our messages on dozens of new websites every day, and push the addresses out before the government can block them. By the time they censor us, we are no longer there. While Big Brother may prevent some basic cyber attacks, they never even see the clever ones. Underground sources are now providing us with computer software that will bring this government to its knees.

The Internet, just like a living organism, needs air to breathe. It thrives based only on the open exchange of information. The most likely thing about the future is that it will be ever more wired. Our challenge is to turn better communication into more power for the common man. Human rights battles will continue to be waged in the future, but time is on our side. If the government continues to strangle the development of the Internet in our country, the end result will be death to the economy, and then death to the state. Either way, we win.

Cyber Resistance

The Internet has done more for the cause of freedom than any technology in history, for both activists and for ordinary citizens. Traditional media pale in comparison, as the printing press and radio are much more susceptible to government control.

However, we still have much to fear. The reports from Minsk are not encouraging. There are no magic bullets, only hard work ahead. Even under our new government, the rights of the people to live in privacy and peace will have to be balanced with legitimate law enforcement powers. As an immediate goal, negotiations should push for transparency. The government must explain everything it is doing, and why.

Retain a high degree of skepticism regarding everything you see on the Internet. Increase vigilance at key times such as elections. Truth is hard enough to find in the real world. In cyberspace, it is ten times harder. Cyber proof may require that you already know the answer to the question you are asking, or that you verify what you find from second source.

A freedom fighter, a terrorist, and a government agent walk into an Internet chat room. Which of them emerges alive? The only way to know for sure is to arrange a meeting in real life!

Resistance Tools

If I tried to offer you one specific cyber solution, the government would subvert it and use it against us. Revolutionary corps cadres are studying dozens of strategies to provide us with both information and anonymity. Here are some of the basic tools:

- Direct access to foreign ISPs
    - Telephone, Web, Satellite
- Anonymous email correspondence
    - Remailers, RSS Mailer
- Anonymous Web browsing
    - PZP, Proxy servers, Encryption
- Dead drops in cyberspace
    - Saving information at a prearranged location
- Steganography
    - Hiding truth among the lies
- Covert channels
    - Normal activity at unusual times
- Common hacker tools
    - Cyber magic in a box
- Out of the box thinking
    - Saving text as pictures

New tools are frequently released. A recent program called Psiphon is specifically designed for information gathering in countries like ours. It is easy to use, and should be difficult for governments to discover. Here is how it works: a computer user in a free country installs Psiphon on his computer, then passes a comrade in a country like ours connection information, including a username and password, usually by telephone or posted mail. The censored user can then open an encrypted connection through the first user's computer to the Internet. This type of communication is difficult for the government both to target and to decipher.

No single strategy or tool will provide us a perfect solution, because the Internet will never behave exactly as anyone, including the government, would like. One final warning: if you feel that you are personally being targeted by Big Brother, lay low. You may already be in a position where very little can help you.

The Future

Our understanding of world affairs and human rights is growing dramatically, especially in the Internet era. In the future, hopefully it will be impossible to enslave or even to fool millions of people. The Internet may be our ticket out of here, so we must try to master it.

Big Brother has many advantages over the people, in brute force and in technology. His tools are everywhere, and they are more precise than ours. Still, the government is also constrained by the limits of technology, which are considerable.

Always be suspicious of Internet outages. Try to understand whether the government is targeting the population as a whole, or you personally. Is the information you seek known to the government? Are there key words that spies could find? You will have to answer the most important question for yourself: does the information you seek not exist, or was the government keeping it from you?

Informants

"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