GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

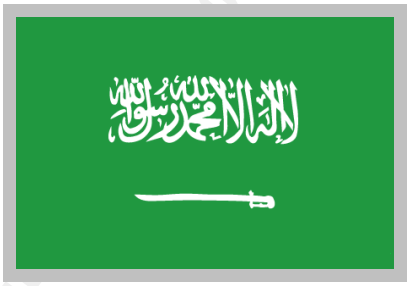
Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Sex, Lies, and Cyberspace: Behind Saudi Arabia's National Firewall



Donne-lui tout de même à boire, dit mon père.
–Hugo

Kenneth Geers

GSEC Version 1.4

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

ABSTRACT

This paper examines the attempt by Saudi Arabia to radically limit where its citizens may go on the Internet. With a rationale based on a mix of morality and politics, the Saudi government has built a national-level proxy server and firewall to filter all Web content and block anything its censors deem "inappropriate." The system caches copies of officially approved websites on servers in-country, where Saudi users can access them second-hand. However, many websites are forbidden. When users try to access sites which have not yet been evaluated, these requests are sent to cyber-triage, where American-made software peruses them for prohibited words before the access request is executed. The theoretical and practical difficulties of cyber-censorship are addressed, and a case study of the fight between a dissident website and the Saudi authorities is used to illustrate the war for Saudi public opinion that is being waged on the Internet. Specific examples of prohibited material give the reader a taste for the kinds of information typically unavailable to Web surfers in the Kingdom. They include many of the most popular websites in the West.

The second half of this paper discusses some of the technologies that exist which can circumvent or even punch a hole right through the Saudi national firewall. They include international telephone calls to foreign Internet Service Providers (ISPs), playing tricks with Internet protocols, use of pseudonymous e-mail accounts and remailers, direct-to-satellite access, and peer-to-peer networking. Three strategies for secreting computer data from one point to another are covered in more detail: anonymous proxy servers, encryption, and steganography. The strengths and weaknesses of each are mentioned, but it is important to note that none of them is perfect. This paper cannot recommend any tools to Saudi Web users, due in part to the fact that prisons in Saudi Arabia are said not to have air-conditioning. These techniques may help Internet users if they are not already under surveillance, but will not help much if a user's communications are being targeted.[1] Finally, a word is said about the relative success of the Saudi mission to protect its Internet users from "inappropriate" material, and about how this goal may not be compatible with the continued economic development of the country.

[1] "How Users can Protect their Rights to Privacy and Anonymity."
URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

© SANS Institute 2000 - 2005 Author retains full rights.

SAUDI ARABIA AND THE INTERNET

If you work for a large enough company, chances are you cannot search for pornography, gamble, or engage in many other types of licentious on-line behavior while on the job. In the USA, you must satisfy these appetites in the privacy of your own home. But in certain countries, like the Kingdom of Saudi Arabia, the government has decided to prevent users from visiting what it considers "inappropriate" sites from anywhere within its borders, at any time, in public or private spaces. The conservative nature of the Saudi government dictates that much of what the West sees on the Internet everyday should not be allowed into the Kingdom uncensored.[2]

Content-filtering on this scale is a monumental task. To accomplish it, the Saudi government built a behemoth national proxy server called the King Abdul-Aziz City for Science and Technology, or KACST, whose goal is to examine all Internet traffic in the country for its "appropriateness." In general, KACST prohibits anything contrary to Muslim values, traditions, or culture.[3] Internet Service Providers are required to conform to these rules, or they do not get an operating license.[4] This is easier to enforce in the Middle East than in the West because the entire telecommunications network, to include international gateways, are owned and operated by the government.[5]

CENSORSHIP IN CYBERSPACE

Saudi Arabia is home to some of the most educated citizens in the Arab world. Saudis routinely communicate with each other and with the outside world on a modern and sophisticated telecommunications infrastructure.[6] The Kingdom has been connected to the Internet since 1994, but access was

---

[2] Gardner, Frank. "Saudis 'defeating' internet porn."
URL: http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm

[3] Whitaker, Brian. "Saudis claim victory in war for control of web." *The Guardian*, 11 May, 2000.
URL: http://www.al-bab.com/media/articles/saudi000511.htm

[4] "Saudi Arabian Response and Reasoning."
URL: http://courses.cs.vt.edu/~cs3604/lib/Censorship/International/Fall01/saudi.html

[5] "Cybercensorship: Its Various Forms." The Internet in the Mideast and North Africa: Free Expression and Censorship.
URL: http://www.hrw.org/advocacy/internet/mena/censorship.htm

[6] Dobbs, Michael. "Online Agitators Breaching Barriers in Mideast: London-Based Saudi Dissidents and Fugitives Find Ways Around Government Censorship." *Washington Post Foreign Service*, October 24, 2001; Page A10.
URL: http://www.library.cornell.edu/colldev/mideast/agitat.htm

© SANS Institute 2000 - 2005 Author retains full rights.

restricted to state, academic, medical, and research facilities until 1999.[7] Today, home accounts are widespread, and there are hundreds of cyber cafes in the country. Men and women are both active Web surfers, and their average daily time online is over three hours.[8]

Initially, Saudi Internet users were offered services such as al-Naseej (www.naseej.com.sa). Al-Naseej provided domestic and international e-mail access, links to domestic databases, and subscriber-only chat rooms. What al-Naseej did not provide was access to the World Wide Web.[9] Now, Internet users can venture out into cyberspace whenever they want, but what they are allowed to do and see there is closely controlled by the government.

The amount of data processed by KACST is so great that the system took two years and a huge budget to build. But due to the sensitive nature of the mission it would fulfill, the whole project was made to fit under one roof. Technicians are imported from places like the USA and Scandinavia,[10] but the censors handing out directives regarding what Web content to block are exclusively Saudi Arabian.[11]

KACST is analogous to a national post office through which all correspondence must travel. In theory, one group of postal inspectors is then sufficient to keep an eye on the entire country. And even though electronic data is unlike traditional mail in that it is broken into small packets to increase the speed with which it can travel through cyberspace, these packets are easily reassembled for inspection at KACST with the aid of eavesdropping software tools.[12]

There are now dozens of private ISPs in Saudi Arabia,[13] but KACST is the country's only officially sanctioned link to the World Wide Web, and all

---

[7] Gavi, Susan. "Crossing Censorship Boundaries." Online Journalism Review. The Middle East Online. Posted: 1999-11-24. Modified: 2002-04-04.
URL: http://www.ojr.org/ojr/technology/1017967030.php

[8] "The China Post: Saudi Arabia to double number of banned sites." May 01 2001:
URL: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356717&rel=true

[9] "The Internet in the Mideast and North Africa: Free Expression and Censorship." Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

[10] Gardner, Frank. "Saudis 'defeating' internet porn."
URL: http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm

[11] "SafeWeb Doubles Usage, Blocked By Saudis." December 19, 2000.
URL: http://siliconvalley.internet.com/news/print.php/540131

[12] "How Users can Protect their Rights to Privacy and Anonymity."
URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

[13] "The Internet in the Mideast and North Africa: Free Expression and Censorship." Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

© SANS Institute 2000 - 2005 Author retains full rights.

prospective ISPs must agree to route their traffic through the KACST gateway.[14] KACST sits at the top of the cyber food chain: it sets Internet access prices, maintains the list of banned websites, and runs firewalls to keep the whole system secure.[15]

From the beginning, Saudi Arabia's goals were ambitious. KACST's president, Saleh Abdulrahman al-'Adhel, said that before the switch to the Internet was officially turned on, KACST would try to eliminate all of the Internet's negative aspects.[16]

KACST overseers, however, eventually realized that they could not accomplish these goals without also regulating the behavior of individual users. Therefore, they specifically forbade the sending or receiving of encrypted information, and the sharing of usernames and passwords.[17]

KACST EXAMPLE FROM THE RIPE WHOIS DATABASE: KING FAHD UNIVERSITY

inetnum:	XXX.26.0.0 - XXX.26.4.255
netname:	KFUPM-1
descr:	King Fahd Univ
country:	SA
admin-c:	NAH3-RIPE
tech-c:	RAT4-RIPE
status:	ASSIGNED PA
mnt-by:	KACST-ISU-MNT
mnt-lower:	KACST-ISU-MNT
changed:	ipreg@saudinic.net.sa 19980209
changed:	hostmaster@ripe.net 19980303
changed:	ipreg@saudinic.net.sa 20010514
changed:	ipreg@saudinic.net.sa 20010707
source:	RIPE

[14] "Losing the Saudi cyberwar." *Guardian Unlimited*, Monday February 26, 2001. URL: http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,443261,00.html

[15] "Saudi Arabian Response and Reasoning."
URL: http://courses.cs.vt.edu/~cs3604/lib/Censorship/International/Fall01/saudi.html

[16] Ibid.

[17] "The Internet in the Mideast and North Africa: Free Expression and Censorship."
Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

© SANS Institute 2000 - 2005 Author retains full rights.

HOW THE SYSTEM WORKS

Saudi authorities are loathe to reveal any technical details relating to KACST's work,[18] but insiders report that KACST evaluates popular Internet sites, then officially sanctions those deemed acceptable, which it caches in a 500-gigabyte storage system. These are accessed quickly by Saudi users because they are only copies of the real websites, and are stored in-country. Specific software applications are not prohibited in the Kingdom per se. For example, KACST explained that Internet chat programs are allowed unless the software in question is specifically linked to the distribution of pornography.[19]

Thus, Saudi Arabia's first line-of-defense on the Internet is a list of banned URLs that are explicitly denied when entered in a browser window.[20] When a user attempts to visit a website that has not been evaluated by KACST reviewers, a second stage of the content-filtering system is activated. Software examines the stream of requested data for anything that matches specific criteria, one of which is the presence of a "stop word" on the homepage.[21] Anything on the list of banned topics will stop the requested information from getting through the KACST proxy server. There are at least thirty categories of prohibited information,[22] and the number of banned sites goes well into the hundreds of thousands.[23]

When access to a site is declined, either because its URL is already on the banned list, or it is found to contain objectionable material, a pop-up warning window appears on the screen. It informs the user in both Arabic and English, "Access to the requested URL is not allowed!"[24] Further, KACST notifies the user that all Web requests are logged.[25] The second warning is not

---

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] "Government-Imposed Filtering Schemes Violate the Right to Free Expression." URL: http://www.hrw.org/advocacy/internet/mena/filters.htm

[22] "Losing the Saudi cyberwar." *Guardian Unlimited*, Monday February 26, 2001. URL: http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,443261,00.html

[23] "The China Post: Saudi Arabia to double number of banned sites." May 01 2001: URL: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356717&rel=true

[24] Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001.
URL: http://www.websense.com/company/news/companynews/01/111901.cfm

[25] Gavi, Susan. "Crossing Censorship Boundaries." Online Journalism Review. The Middle East Online. Posted: 1999-11-24. Modified: 2002-04-04.

© SANS Institute 2000 - 2005 Author retains full rights.

unimportant, because government eavesdroppers can, with an IP address, find the computer terminal in question, and depending on the nature of the incident, the police might show up at his or her door. It is true that it can be more difficult to find the person who was sitting at the keyboard at the time of the request, but that is why in countries like Saudi Arabia, publicly available Internet terminals that allow for easy, anonymous web surfing, are scarce.[26]

The two-stage system described above is the one advertised by the Saudi government. However, there do exist more stifling approaches to censorship, such as the use of a "whitelist", of which the Saudi government has been accused. Blacklists ban certain books or websites because they are flagged by censors as containing inappropriate content. But with whitelists, KACST software would be configured to disallow everything but that which is explicitly allowed.[27] In other words, there would be no need for a second stage to the KACST system. When users attempted to visit unfamiliar webpages, they would simply be out of luck. Some reporting has quoted "industry insiders" claiming that KACST has used a whitelisting strategy in the past. According to these sources, an internal KACST committee officially sanctioned a list of "desirable" sites, and all others were banned by default.[28]

It is beyond the scope of this paper, but worth mentioning, that KACST has the capability – and mandate – to do far more than simple website content filtering. While Saudi users have found some interesting ways to avoid e-mail monitoring (discussed below), KACST employees often can read, block, and delete e-mail messages based on e-mail address, Internet Protocol (IP) address, or character strings in the message itself. If string analysis perceived that "royal family" and "corrupt" were in the same sentence, the message could be flagged for closer inspection. At that point, KACST might choose to do something with the message other than deliver it. It is possible that such information could be passed to law enforcement authorities.[29]

AMERICAN COMPANIES BEHIND THE VEIL

At least ten companies from the United States, Britain, Germany, and the

URL: http://www.ojr.org/ojr/technology/1017967030.php

[26] "How Users can Protect their Rights to Privacy and Anonymity."
URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

[27] "Government-Imposed Filtering Schemes Violate the Right to Free Expression."
URL: http://www.hrw.org/advocacy/internet/mena/filters.htm

[28] "The Internet in the Mideast and North Africa: Free Expression and Censorship."
Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

[29] "How Users can Protect their Rights to Privacy and Anonymity."
URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Netherlands have contracted with Saudi authorities to provide KACST's infrastructure. Symantec, Websense (whose clients include the U.S. Army), Surf Control, and N2H2 are all on the payroll, but the company primarily responsible for filtering Web content is Secure Computing of San Jose, California.[30]

Secure Computing's software is called SmartFilter, and it has been in place since Saudi Arabia officially connected to the Internet in February 1999. SmartFilter ships with default content categories like pornography and gambling, but it was selected by KACST due to ease of customization. It is crucial to KACST's mission that it be able to quickly identify material offensive to Islam or to the Saudi royal family, and block it.[31]

Privacy advocates have criticized the software companies that create such tools, but industry representatives counter that their products are politically neutral. A sales executive for Secure Computing explained that "Once we sell them the product, we can't enforce how they use it."[32]

SmartFilter's mandate will expire in 2003, and competition is intense for the follow-on contract.[33] Most of the companies in the running are American. They are not only interested in the multi-million-dollar deal itself, but also in the name recognition that would inevitably come from winning the award. The winner should have the upper hand in negotiating contracts from other countries interested in determining "appropriate" content for their Internet users.[34]

KACST is encouraging healthy competition: Dr. Eyas S. al-Hajery, a KACST director, coyly says "It's not that we are unhappy with the product, we're just looking for a better solution."[35] So the competitors are slashing their prices, and one German company is said to have offered the service for free. All the companies are working to make software that is Arabic-language friendly, customizable, and impenetrable to anything un-Islamic or anti-Saudi.[36] Websense has already begun a software trial, and is considered a top contender to win the award.[37]

---

[30] Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001 .
URL: http://www.websense.com/company/news/companynews/01/111901.cfm

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

© SANS Institute 2000 - 2005 Author retains full rights.

PORNOGRAPHY TO POLITICS: A CASE STUDY

Pornography is the first topic Saudi authorities bring up when questioned about Internet censorship. And vis-à-vis pornography, KACST's leadership contends that the battle is being won. Its director claims that all major pornographic sites have been identified and blocked.[38]

But close inspection indicates that Saudi Arabia's efforts are based in politics as much as they are in morality. KACST has clearly been tasked with monitoring and censoring the exchange of information that might affect the well-being of the Saudi royal family or its government.[39]

A case in point is the battle that has been waged with a London-based dissident group called the Movement for Islamic Reform in Arabia (MIRA). MIRA is a political organization, not a distributor of pornography. But because MIRA is implacably opposed to the current Saudi government, KACST was instructed to add MIRA's IP address to its list of banned websites. So any information MIRA puts out, whether true or false, is not supposed to enter the Kingdom. There can be no doubt about the Saudi government's intention here, witness the cat-and-mouse game which followed.

When MIRA's IP address was found to have been blocked by KACST, which was apparent in MIRA's weblogs, the group decided to change its IP to one that was not on KACST's list of banned sites. Immediately, MIRA was again accessible in the Kingdom (it is unknown why the second stage of KACST's system was not able to block the website based on content). But the new IP eventually became widely known, and KACST blocked it again. This process repeated itself many times over. MIRA would pick a new IP, then KACST would block it. On average, MIRA was available for about a week. MIRA's challenge was to make interested Saudi citizens aware of its new Web address before the block was in place again.[40]

Not satisfied with this protracted game of hide-and-seek, in which its new IP address was always eventually found and blocked by KACST, MIRA's webmasters developed a more effective, two-pronged solution. First, the MIRA website (www.islah.org)[41] added randomization of port numbers to its new IP

---

[38] Gardner, Frank. "Saudis 'defeating' internet porn."
URL: http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm

[39] "The Internet in the Mideast and North Africa: Free Expression and Censorship." Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

[40] "Losing the Saudi cyberwar." *Guardian Unlimited*, Monday February 26, 2001. URL: http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,443261,00.html

[41] Dobbs, Michael. "Online Agitators Breaching Barriers in Mideast: London-Based Saudi Dissidents and Fugitives Find Ways Around Government Censorship." *Washington Post*

© SANS Institute 2000 - 2005 Author retains full rights.

addresses. This added twist made it more difficult for KACST to do its detective work, since the Web requests leaving Saudi Arabia were not necessarily headed for port 80. Thus, without much work, www.islah.org added over 64,000 possible Web addresses (equal to the number of available ports) to every one of its new IP addresses.

Second, MIRA developed an efficient way to communicate the current iteration of its Web address to Saudi citizens, in the form of an automatic reply from islah@islah.org. Prospective website visitors sent a blank e-mail and waited for the reply, which would arrive in seconds. From Saudi Arabia, the blank e-mails were typically sent via webmail such as Hotmail or Yahoo!, whose login process made it impossible for KACST software to see where the e-mails were going, or what information they contained.[42]

According to MIRA's head, Dr. Saad Fagih, after these changes were implemented the number of hits to his site reached 75,000 a day. He says that KACST eventually decided to abandon its efforts to block the site, perhaps in part due to the name recognition MIRA achieved, and in part due to the technical difficulties which MIRA had imposed on KACST. Dr. Fagih revealed that his technicians were able to hack into KACST computers and verify the Saudi surrender.[43]

These days, Dr. Fagih interacts with his followers in Saudi Arabia via live Internet chat sessions. He delivers audible cyber lectures twice a week from his home in London. Hundreds of people in Saudi Arabia log on and ask him questions about his organization and its political bent. MIRA's chat rooms have become so popular that Saudi authorities are believed to have infiltrated them on counterintelligence missions. Dr. Fagih said that one user, "Tarik2001," who he thinks is a government agent, posted a message quoting a Washington Post article that never existed: "Saudi dissident Saad al-Fagih has died in a car accident in London."[44]

Indeed, it is thought that many different Saudi security agencies have a role to play in the country's effort to control the Internet within its borders. MIRA's www.islah.org is far from the only politically-affiliated site affected. Others have included www.cdhrap.com, the Committee for the Defense of Human Rights in the Arabian Peninsula, and www.saudhouse.com, by the Committee Against Corruption in Saudi Arabia.[45] Beyond politics, history is

---

Foreign Service, October 24, 2001; Page A10.
URL: http://www.library.cornell.edu/colldev/mideast/agitat.htm

[42] "Losing the Saudi cyberwar." *Guardian Unlimited*, Monday February 26, 2001. URL: http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,443261,00.html

[43] Ibid.

[44] Dobbs, Michael. "Online Agitators Breaching Barriers in Mideast: London-Based Saudi Dissidents and Fugitives Find Ways Around Government Censorship." *Washington Post Foreign Service*, October 24, 2001; Page A10.
URL: http://www.library.cornell.edu/colldev/mideast/agitat.htm

© SANS Institute 2000 - 2005 Author retains full rights.

important in the Middle East, so some sites that recount "unofficial" histories of Saudi Arabia are also blocked.[46]

CHICKEN BREASTS AND MIDDLESEX COUNTY

To censor the Internet at all is not an easy task. But to censor the Internet website by website, based on its pages' moral and political content, is especially tricky because it is so difficult to sort the wheat from the chaff. There is no software available today that can really understand even the simplest op-ed in today's New York Times. Recognizing words is one thing, understanding how they are used by an author in a given sentence or article is quite another. There is no doubt that KACST software will block access to material that looks like a duck and walks like a duck, but in fact is not even close to being a duck.

The problem with using prohibited "stop-words" to block access to information on the Web is that computers are not smart enough to know the difference between a good recipe for marinated chicken breasts and a woman's breasts. Banning access to information about sex throws the baby out with the bathwater. Licentious sexual material is blocked, to be sure, but so is medical advice on how to avoid sexually-transmitted diseases (STDs).[47]

The decision to censor information at all usually leads to over-censorship.[48] Some available software, for example, is only smart enough to block access to a given server, even though there may only be one web site on that server which contains pornography.[49] Knowing that, an attacker could target a website with a denial-of-service by poisoning its server with prohibited material.

Saudi authorities insist that they are trying to be reasonable when they decide which sites to ban. KACST provides forms for users to request both additions to and removals from the blacklist, and claims that over 500 requests are received every day recommending that certain websites be banned. Of these, about half are subsequently blacklisted. At that rate, 7,000 sites a month are added to the list.

---

[45] "The Internet in the Mideast and North Africa: Free Expression and Censorship." Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

[46] Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001 .
URL: http://www.websense.com/company/news/companynews/01/111901.cfm

[47] "Government-Imposed Filtering Schemes Violate the Right to Free Expression."
URL: http://www.hrw.org/advocacy/internet/mena/filters.htm

[48] Whitaker, Brian. "Saudis claim victory in war for control of web." *The Guardian*, 11 May, 2000.
URL: http://www.al-bab.com/media/articles/saudi000511.htm

[49] "Government-Imposed Filtering Schemes Violate the Right to Free Expression."
URL: http://www.hrw.org/advocacy/internet/mena/filters.htm

© SANS Institute 2000 - 2005 Author retains full rights.

On the other hand, KACST says over 100 requests come in each day to remove sites from the list as well. In general, this is because users feel that the sites in question have been mischaracterized by the content-filtering software. No statistics were offered on how many of the 100 are typically unblocked.[50]

Secure Computing dismisses the criticism of over-censorship altogether, arguing that all banned websites are eventually double-checked by real people who make sure that the SmartFilter software is doing its job correctly. For example, in August 2000 the decision was made to block Yahoo! chat rooms wholesale, because the topics discussed in them were so often of a sexual nature. But enough Saudis were dismayed by the decision that KACST eventually began to selectively unblock chat rooms that clearly had nothing to do with sex. The catalyst in this case was the widespread use of the user request forms described above.[51]

In the end, pornography may be easier to censor than politics. Vulgar sex words can simply be weeded out of Internet traffic, but software cannot readily determine whether a political article was written with a view toward supporting or opposing a certain political figure or act. It only knows that political keywords exist in a given text. Even a Finnish computer geek sitting in his cube farm at KACST will find this task difficult. If it is undertaken at all, it must be done by true subject matter experts (SME) who speak the local language fluently. Practically speaking, that would be far too time-consuming and expensive a process to be of much help for the citizens of Saudi Arabia.

One independent study, undertaken at Harvard University, conducted an experiment to gauge the scope of KACST's content-filtering system. A software program was written to make 60,000 Web requests from a proxy server in Saudi Arabia. 2,038 of them were blocked. The information contained on the inaccessible webpages included information on religion, health, education, humor, and entertainment. Also included were general reference works. *Rolling Stone* magazine, www.ivillage.com, and the "Women in American History" section of *Encyclopedia Britannica Online* had all been blacklisted.[52]

From other sources, we know that political activist sites like Amnesty International are forbidden,[53] as well as information on computer hacking, which obviously could give Saudi citizens an upper hand in figuring out how to beat the system.[54]

---

[50] Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001 .
URL: http://www.websense.com/company/news/companynews/01/111901.cfm

[51] Ibid.

[52] "Internet Filtering in Saudi Arabia" (University Project):
http://cyber.law.harvard.edu/filtering/saudiarabia/

[53] Whitaker, Brian. "Saudis claim victory in war for control of web." *The Guardian*, 11 May, 2000.
URL: http://www.al-bab.com/media/articles/saudi000511.htm

© SANS Institute 2000 - 2005 Author retains full rights.

It must be said, however, that the very nature of the Internet should always keep KACST a step or two behind the curve. No matter how good its software, computer scientists, and censors are, the Internet evolves so rapidly that Saudi Arabia – or any other nation or corporation – will never be morally or politically pure. Saudi officials have publicly acknowledged that it is hard to keep up. New websites appear on the Internet every hour of every day, and each one of them is potentially anti-Muslim and anti-Saudi.[55]

FEAR AND SELF-CENSORSHIP IN ARABIA

In an authoritarian country like Saudi Arabia, part of the national firewall will always be self-censorship on the part of ordinary citizens. Government intimidation in non-democratic countries inhibits both what is published and what is discussed even behind closed doors.

No Middle Eastern government has admitted to reading the e-mail of its people, but communication via the Internet is highly vulnerable to surveillance and interception – especially when every bit of data flows through one, state-owned gateway. In Saudi Arabia, there have been reports of e-mail inexplicably disappearing, or taking two or three days to reach the recipient's inbox.[56]

In neighboring Jordan – a freer country than Saudi Arabia by far – two people were detained by police in 1996 for comments posted on the Internet. In Bahrain, a telecommunications engineer was questioned in 1997 over allegations by informants that he was sending information to opposition groups via the Internet.[57]

The U.S. State Department reports that most countries in the Middle East monitor the telephone conversations of their citizens, usually without any warrants or judicial supervision.[58] Reading e-mail is just as easy as intercepting telephone conversations. If the police have access to your phone line, they can use readily available software to reassemble the discrete data packets and read your correspondence. They can also serve a warrant to your ISP for its logs, or simply require your ISP's employees to do their surveillance work for them.[59]

---

[54] Gavi, Susan. "Crossing Censorship Boundaries." Online Journalism Review. The Middle East Online. Posted: 1999-11-24. Modified: 2002-04-04.
URL: http://www.ojr.org/ojr/technology/1017967030.php

[55] Gardner, Frank. "Saudis 'defeating' internet porn."
URL: http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm

[56] "Cybercensorship: Its Various Forms." The Internet in the Mideast and North Africa: Free Expression and Censorship.
URL: http://www.hrw.org/advocacy/internet/mena/censorship.htm

[57] Ibid.

[58] Ibid.

[59] "How Users can Protect their Rights to Privacy and Anonymity."

© SANS Institute 2000 - 2005 Author retains full rights.

PENETRATING THE SAUDI FIREWALL

Saudi Arabians have found many ways to obtain forbidden information and to communicate surreptitiously through and around the KACST national firewall. At the low-tech end, wary users access the Internet simply by using computer terminals and e-mail accounts that they assume are not being monitored, usually with the help of someone they trust.[60]

A step up from there are international telephone calls to foreign ISPs. These long-distance dial-up connections are expensive, but they can give the caller unrestricted access to the Internet,[61] because the Saudi monitoring system is wholly bypassed.[62] The average price of a call to Europe or to the U.S. is about $2.00 a minute, but tens of thousands of Saudis have connected to the Internet in this fashion. In general, Saudi Arabia does not restrict the sale of modems.[63]

Dissident websites have a number of options at their disposal. Some, like www.islah.org, have changed their IPs periodically. Others Web masters have "mirrored" their content at WWW sites whose addresses are not on KACST's blacklist. Webpages can also be sent by e-mail to friends or entire list-serves using html or as attached files.[64]

There are many creative ways to send e-mail. Web-based, pseudonymous accounts like Hotmail, Yahoo!, and Web@ddress have been popular in Saudi Arabia, since they are free and do not require users to register with a real name.[65] Remailing services have been used to provide an additional

---

URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

[60] Ibid.

[61] Whitaker, Brian. "Saudis claim victory in war for control of web." *The Guardian*, 11 May, 2000.
URL: http://www.al-bab.com/media/articles/saudi000511.htm

[62] Gardner, Frank. "Saudis 'defeating' internet porn."
URL: http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm

[63] "The Internet in the Mideast and North Africa: Free Expression and Censorship."
Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

[64] "Cybercensorship: Its Various Forms." The Internet in the Mideast and North Africa: Free Expression and Censorship.
URL: http://www.hrw.org/advocacy/internet/mena/censorship.htm

[65] "How Users can Protect their Rights to Privacy and Anonymity."
URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

© SANS Institute 2000 - 2005 Author retains full rights.

layer of anonymity. Remailers forward data across the Web only after stripping it of all information that could identify the sender. They typically keep no weblogs of the traffic they pass on, and often send the data to another remailer or two before it reaches the recipient's inbox. Encryption is used to further obfuscate the communication en route. If done correctly, the authorities only know that you visited a remailer site; they would not have a copy of your message, see the address of the recipient, or even know whether the message had been encrypted before being sent.[66]

A growing trend in the Middle East is the acquisition of direct-to-satellite Internet access. The dishes required are small enough that they fit discreetly on a balcony or rooftop. The connections they establish to the World Wide Web allow users to bypass the national, ground-based telecommunications system altogether. Currently, this type of Internet access is too expensive for most users, but prices are falling, and in the future this technology will pose a challenge to any country wanting to control its national borders in cyberspace.[67]

Cutting edge software will always push the envelope further and make KACST's job harder. Peer-to-peer networking, for instance, has awesome potential. A group of democracy-loving hackers called Hacktivismo is developing peer-to-peer freeware that is designed and may be destined to shoot giant holes in Internet censorship worldwide, by governments or companies. It is called Six/Four, to commemorate the date of the Chinese government's 1989 crackdown in Tiananman Square. Using virtual private networking (VPN) technology, Hacktivismo hopes to make file-sharing between computer users completely invisible to firewalls and content-filtering systems like that used by KACST. It is due to be released in late 2003.[68]

Below, this paper describes in more detail three methods that Saudi Internet users have employed to keep their Web activity hidden from KACST oversight. Again, no tools can be recommended here, both because none of them is perfect, and because this is a public forum. If personal communications are being specifically targeted by the authorities, few commonly available tools offer any help at all.[69]

ANONYMOUS PROXY SERVERS

---

[66] Ibid.

[67] Ibid.

[68] Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001 .
URL: http://www.websense.com/company/news/companynews/01/111901.cfm

[69] "How Users can Protect their Rights to Privacy and Anonymity."
URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Anonymous proxy servers were designed with the express intent of giving users in countries like Saudi Arabia equal access to the wonders of the World Wide Web.[70] The technology is entirely Web-based. A proxy server takes the URL you type into a browser window, encrypts it, and then makes the Web request on your behalf. It accomplishes that task by swapping your IP address for its own, and swaps it back again once it has received the requested data. In other words, it communicates with the Web server in question for you. Anonymous proxy servers are also designed to block pop-up windows and third-party cookies, and they can even explain to you what the intercepted cookies were trying to accomplish. Last but not least, there are no downloads required.[71]

Saudi Web surfers have made ample use of this technology.[72] One estimate suggests that nearly half of all Saudi Internet users have employed foreign-based proxy servers to connect to websites that were banned by KACST. Most of these either contained pornography or information critical of Saudi Arabia.[73]

From KACST's perspective, allowing its users to visit anonymous proxy servers is tantamount to surrendering its control of the Internet in Saudi Arabia. That is obviously untenable to upper management. So when the IP addresses of such servers are found, they are added to the list of banned websites.[74] KACST employees must further work to prevent the kind of workarounds that MIRA has developed for its website. KACST has found and blocked at least three mirror sites of a popular anti-censorship proxy server called Osiris.[75]

One proxy service that became very popular in the Kingdom is called Safeweb. Saudis used it to enter prohibited chat rooms and read international news.[76] Its IP was eventually blocked, but Safeweb developers are working on a

---

[70] "SafeWeb Doubles Usage, Blocked By Saudis." December 19, 2000.
URL: http://siliconvalley.internet.com/news/print.php/540131

[71] Ibid.

[72] Dobbs, Michael. "Online Agitators Breaching Barriers in Mideast: London-Based Saudi Dissidents and Fugitives Find Ways Around Government Censorship." *Washington Post Foreign Service*, October 24, 2001; Page A10.
URL: http://www.library.cornell.edu/colldev/mideast/agitat.htm

[73] "The China Post: Saudi Arabia to double number of banned sites." May 01 2001:
URL: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356717&rel=true

[74] "SafeWeb Doubles Usage, Blocked By Saudis." December 19, 2000.
URL: http://siliconvalley.internet.com/news/print.php/540131

[75] "The Internet in the Mideast and North Africa: Free Expression and Censorship." Human Rights Watch.
URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

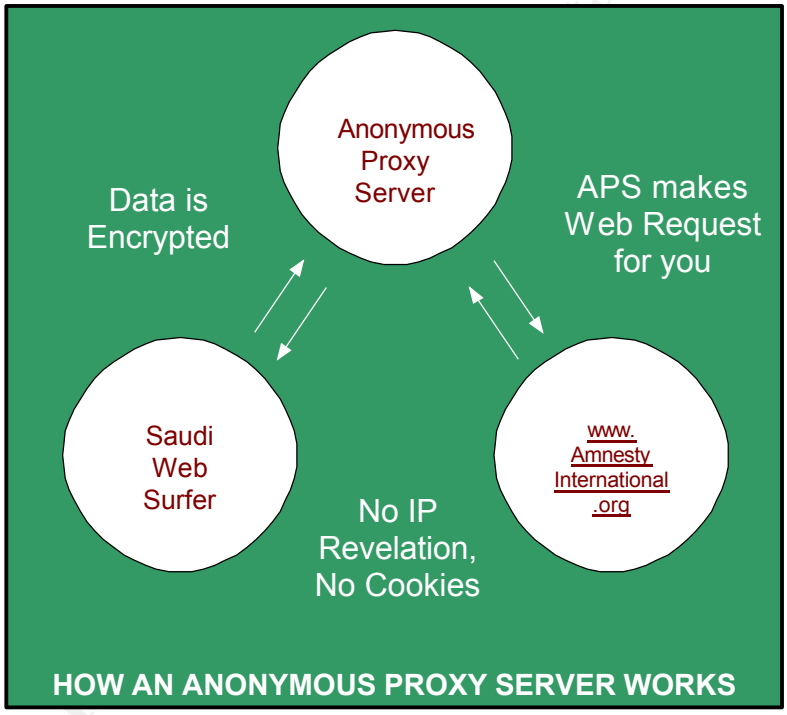
[76] "SafeWeb Doubles Usage, Blocked By Saudis." December 19, 2000.
URL: http://siliconvalley.internet.com/news/print.php/540131

© SANS Institute 2000 - 2005 Author retains full rights.

new version of its software, whose aim is to prevent any government or company from blocking access to its services.[77]

Anonymizing technology is not perfect. Typically, it cannot guarantee that your identity will remain anonymous to the anonymizing service itself, or to your own ISP. The latter is clearly a major problem for Saudi users.

Privacy advocates and their software developers are working on these larger theoretical issues as well. One solution, called "Crowds," is designed to work by grouping Web requests from different users into a larger pool. The idea is to further obscure individual requests, to make it more difficult for Web servers, eavesdroppers, and even other "Crowd" members from associating a particular request with its requestor.[78]



ENCRYPTION

Strong encryption is reliable and cheap. Pretty Good Privacy, or PGP, can be downloaded in seconds for free (or carried into the country via floppy disk), and stored on your personal computer. PGP is based on Public Key

[77] Ibid.

[78] "How Users can Protect their Rights to Privacy and Anonymity." URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Infrastructure (PKI) concepts. It couples a sophisticated algorithm with a secret passphrase to encrypt data, and is so powerful that it has come to play an important role in human rights campaigns around the world. Victims, witnesses, and political dissidents have relied on its power to tell their stories in confidence. They can even sign cryptographic, digital signatures to help verify the authenticity and integrity of their stories.[79]

Theoretically, any encryption scheme can be broken when the code breaker has enough time, expertise, and computing power at his or her disposal. But the great effort required to break good encryption like PGP is prohibitive for practical purposes such as routine monitoring of the Internet. That is why Saudi Arabia, and many other countries, have disallowed the use of encryption without government authorization.[80]

Encryption is not a perfect solution for Saudi Web users, however. While traffic sent across the Internet is indeed indecipherable, the fact that the message has been sent in an encrypted format is readily apparent. The reason is that the file size required to reliably encrypt data is enormous.

Thus, in some countries encryption must be used with trepidation. If it is illegal, an organization like KACST, through the reverse look-up of an IP address, could attempt to identify who is responsible for sending the encrypted traffic. Then, they would likely pass this information along to the police, who would then pay a visit to the residence or workstation in question.

Law enforcement could then either force the user to disclose the contents of certain messages, or demand his or her private key passphrase. Once the private key is known, it can be matched with the user's public key to decrypt any past and future messages, or the government could use the passphrase to impersonate the user with third parties.[81]

PGP Encryption

Directions.txt (Original file written in Notepad):

The train is bound for Cairo.

Directions.txt.pgp (The same file encrypted and digitally signed):

¨_PGPÁÁN_GoU_-è…[__ÿC[Þ,lŠo$(›xË®
_»k¯ÍR_ 3_+\|ã- =_T äÜˆo_(S3ÈC*ƒ*=£”*žö¡þ_õ‹S**”__$
³±__ qð 8êXâF|?¹î j_~½6MX~'ÌTÅ_®Ì_ìË¿}çÙˆðr„mWa„ÿLâø³^èÚ_4ø_P^Ä
Cd&óðð£<_7p_m»*_Ô¼;´Ð ÇêªS¦_!ÇÚeGy_nÐ·_
C^£È_¾-è_Ì_š¯ÇðNõ_º^ù“kº×
û”*Sk_ïŧ“k†¸›;D<‡ñÿ:,& š__._K³ÓéNgãS¬·é†â—RMKø„o²_z³}_f¼ßh_8³_ü_®TâÂáóqwÄì©e_søwŒhý
îª?˜úLR
»¸Ey”Û « ÿ,Pe
h§ëüp“¥×ŒsVx f"tW~Òr«òóì… u'6—êÑc6_Ì¹__^_kl2šˆš_ bÉ§ _ôõ_Ÿ‰
ªGú÷Á_^ðå__ãëÊ UV__ÙÉ†Íyö_Ã0c Q _½õwHýX_7__4?ùÕÔ'³×8¥_"_
šán˜½±h‹¶µ_ýÓž¨Í_ÐiFÔ?ÂP _+% ;Áµu½ìg_m ÔØ‡Jeä·YjŠœ__,ÿÈ,u_
?_lÔ¶ óÖFÌ;bÀœ$=__™#_±ûÛ†W^ö‰(¥ ’_É ƒ)Áy'â_Ìjß“_˜d$¢_á™É_›dM`Rl_»_xOçÀŽ_¬_b Þ_Kç
cçzžƒÐQ ?KÜM_R
Ø(_Û_ï8»RHûn™¡—â_V>‡}©=ÎÊpA#ˆÐ_û_6Àg2œÎ0jCpÊL8___Çà _j˜ÿ_
DoÐý_ñýŒ_ujÀ_?‹4úDÀ®ÔÙÇ9

Directions.txt (Recipient decrypts using secret passphrase):

The train is bound for Cairo.

EGOGPH

STANRAY

eg ogr hy a

St an ap is

[79] Ibid

[80] Ibid

[81] Ibid

© SANS Institute 2000 - 2005 Author retains full rights.

subtler way to slip messages past prying eyes. It solves some of the problems inherent in encryption, such as the transmission of unusually large file sizes. The trick behind steganography is that the secret data is hidden in plain sight. The ones and zeros which compose the data are scattered far and wide among the ones and zeros of other, much larger files. These are usually images, videos, or audio clips.

The intended recipient of the secret message must know where on the Internet to find the "stegged" file, which software tool was used to hide the data, and possibly a secret passphrase before the data can be extracted. Otherwise, the added information will simply appear as an extra fleck of color, or a bit of noise in one of millions of similar files floating around the Internet. To the naked eye, it is essentially invisible.

In the example below, the telephone number and address of a hypothetical Saudi political dissident is hidden in a picture of the King of Saudi Arabia. It was stegged using S-tools. Such a photo could be sent via e-mail to a contact in a foreign country, or posted on the WWW from within the King's own palace. Then, in another country, it can be de-stegged using the same passphrase, which is communicated by some other means.[82]



These two photos of the King have the same appearance and file size, but only one of them has been stegged with secret information.

Steganography is a brilliant way to hide data. However, there are drawbacks. As with any software, steg tools can leave recognizable signatures for which government censors and other snoops are looking. Also, it is possible that the very fact you are sending files large enough to hide other files will arouse suspicion.

[82] Ibid.

© SANS Institute 2000 - 2005 Author retains full rights.

THE FUTURE OF CENSORSHIP IN ARABIA

The national firewall that Saudi Arabia has created to examine all Internet traffic within its borders for moral and political appropriateness has been successful in keeping ordinary Internet users from going to thousands of websites that may be anti-Muslim or anti-Saudi. However, it is impossible for any firewall, particularly one as large as this, to work perfectly. For those who are willing to accept the risks (i.e. getting arrested), there are many ways to try to obtain prohibited information and to communicate in confidence on the Internet.

In the future, Saudi Arabia's attempt to shield its citizens from pornography and differing points of view may be doomed to failure. The reason is economic: KACST is inhibiting the growth of e-commerce. Government monopoly over anything usually entails a high cost in efficiency and vitality. Normally, these are the Internet's strengths, but such strict censorship has slowed progress in cyberspace down to a crawl. One Internet activist put it this way: "There's no possibility of developing e-commerce unless they (Saudi Arabia) allow liberalisation and the growth of independent service providers … It's a choice between surrendering control and being shut off from the electronic future."[83]

Saudi Arabia is already trailing far behind some of its neighbors in developing a legal framework for doing business on the Internet. The bottom line should eventually convince Saudi authorities to relax their apprehensions about cyberspace, even if that means allowing their citizens to subscribe to Playboy magazine and read unflattering articles about the royal family.[84]

The United States could do more to help ordinary Saudis in their quest for Internet freedom, but such an effort has been hampered by politics. China is also trying to shoulder surf its inhabitants on the Internet, but because China is not a U.S. ally, Washington has been indignant, and even announced that it plans to help Chinese citizens circumvent their government's firewall. But Saudi Arabia is politically aligned with the U.S., and thus has been above criticism.[85]

In the big picture, freedom-lovers are optimistic. The Internet is widely acknowledged already to have done more for freedom of expression in the Middle East and elsewhere than any medium in history. Casual Web surfers and hard-core political activists alike have found their thirst for information and

---

[83] Whitaker, Brian. "Saudis claim victory in war for control of web." *The Guardian*, 11 May, 2000. URL: http://www.al-bab.com/media/articles/saudi000511.htm

[84] Ibid.

[85] Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001 .
URL: http://www.websense.com/company/news/companynews/01/111901.cfm

© SANS Institute 2000 - 2005 Author retains full rights.

open discussion slaked more than ever before, in cyberspace.[86]

© SANS Institute 2000 - 2005, Author retains full rights.

[86] Gavi, Susan. "Crossing Censorship Boundaries." Online Journalism Review. The Middle East Online. Posted: 1999-11-24. Modified: 2002-04-04.
URL: http://www.ojr.org/ojr/technology/1017967030.php

© SANS Institute 2000 - 2005 Author retains full rights.

BIBLIOGRAPHY

"The 20 Enemies of the Internet." Radio Free Europe/Radio Liberty. August, 1999. URL: http://www.rferl.org/nca/special/enemies.html

"Arab Media: Saudi Internet Rules." Al-Watan newspaper 21/11/1421 (12 February 2001) URL: http://www.al-bab.com/media/docs/saudi.htm

"Arab youths bypass government's CyberPatrol Net-censorship. (fwd)" To: debate@fitug.de, From: 3umoelle@informatik.uni-hamburg.de (Ulf Möller), Date: Tue, 23 Sep 1997, To: fight-censorship@vorlon.mit.edu, cypherpunks@toad.com, From: Declan McCullagh declan@well.com URL: http://www.fitug.de/debate/9709/msg00037.html

"Censorship in Law and Practice." Computer Professionals for Social Responsibility. Last updated: November 21, 2001. URL: http://www.cpsr.org/cpsr/nii/cyber-rights/web/current-speech.html

"Censorware Companies and Saudi Arabia Censorship." Educational CyberPlayGround: Crisis Curriculum and Resources. URL: http://www.edu-cyberpg.com/Technology/securitycrisisCENSORSHIP.html

"The China Post: Saudi Arabia to double number of banned sites." NUA. May 01 2001. URL: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356717&rel=true

"Cybercensorship: Its Various Forms." Human Rights Watch. The Internet in the Mideast and North Africa: Free Expression and Censorship. URL: http://www.hrw.org/advocacy/internet/mena/censorship.htm

Dobbs, Michael. "Online Agitators Breaching Barriers in Mideast: London-Based Saudi Dissidents and Fugitives Find Ways Around Government Censorship." *Washington Post Foreign Service*, October 24, 2001; Page A10. URL: http://www.library.cornell.edu/colldev/mideast/agitat.htm

Gardner, Frank. "Saudis 'defeating' internet porn." BBC News Online, 10 May 2000. URL: http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm

Gavi, Susan. "Crossing Censorship Boundaries." Online Journalism Review. The Middle East Online. Posted: 1999-11-24. Modified: 2002-04-04. URL: http://www.ojr.org/ojr/technology/1017967030.php

"Government-Imposed Filtering Schemes Violate the Right to Free Expression." Human Rights Watch. URL:

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.hrw.org/advocacy/internet/mena/filters.htm

"How Users can Protect their Rights to Privacy and Anonymity." Human Rights Watch. URL: http://www.hrw.org/advocacy/internet/mena/privacy-rights.htm

"Internet Censorship: law & policy around the world." Electronic Frontiers Australia Inc. 28 March, 2002. URL: http://www.efa.org.au/Issues/Censor/cens3.html#sau

"Internet Filtering in Saudi Arabia" (University Project by Jonathan Zittrain and Benjamin Edelman). (A new and improved version was posted 12 September, 2002) URL: http://cyber.law.harvard.edu/filtering/saudiarabia/

"The Internet in the Mideast and North Africa: Free Expression and Censorship." Human Rights Watch. URL: http://www.hrw.org/advocacy/internet/mena/saudi.htm

Lee, Jennifer S. "Companies Compete to Provide Saudi Internet Veil." *The New York Times*, November 19, 2001. URL: http://www.websense.com/company/news/companynews/01/111901.cfm

"SafeWeb Doubles Usage, Blocked By Saudis." Internetnews.com. December 19, 2000. URL: http://siliconvalley.internet.com/news/print.php/540131

"Saudi Arabian Response and Reasoning." Virginia Tech Department of Computer Science. Professionalism in Computing Digital Library. URL: http://courses.cs.vt.edu/~cs3604/lib/Censorship/International/Fall01/saudi.html

Whitaker, Brian. "Losing the Saudi cyberwar." *Guardian Unlimited*, Monday February 26, 2001. URL: http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,443261,00.html

Whitaker, Brian. "Saudis claim victory in war for control of web." *The Guardian*, 11 May, 2000. URL: http://www.al-bab.com/media/articles/saudi000511.htm

© SANS Institute 2000 - 2005, Author retains full rights.