Global Information Assurance Certification Paper

The "Great Firewall" of China

A Real National Strategy to Secure Cyberspace?

by Carolyn Pearson
SANS GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b, Option 1
May 10, 2004

Table of Contents

Abstract

The so-called “Great Firewall” of China is the structure — largely technological, but also with legal and social components — put in place to prevent use of the Internet in the People’s Republic of China (PRC) for purposes not approved by the government, especially access to content that the government objects to. Though its primary reason for existence is not to provide information security in the sense that this term is normally used in Western countries, the Great Firewall relies on many of the same approaches that are used around the world to combat hacking, online pornography and other types of computer crime. As such, it provides an interesting case study in the large-scale application of information security tools and techniques, and the importance of high-level executive support, user education and enforcement.

The PRC Government’s Motives & Goals

Over the past two decades, the government of the PRC has publicly moved away from traditional communist economic principles, such as collective ownership. The Communist Party, paradoxically, is encouraging and fostering free-market capitalism and private entrepreneurs. The country even joined the World Trade Organization (WTO) in 2001, taking a place at the table with the world’s major capitalist democracies.

To help China participate fully in the world economy, the government is pushing widespread adoption of modern technology, including the Internet. It declared 1996 “The Year of the Internet,” even though fewer than 150,000 Chinese had Internet access at the time. [Barmé & Sang] Since then it has continued to promote use of the Internet, particularly for scientific and business uses, and has reportedly spent billions on Internet infrastructure. [Boyd]

These efforts have been effective. By December 2003, China was second only to the United States in the number of Internet users, with 79.5 million. [Amnesty International, 2004]

Despite its embrace of formerly forbidden economic pursuits, however, the Chinese government does not wish to adopt certain other Western ideas, such as free speech. Criticism of the government is still treated as a serious crime, and public expression of other ideas that the government does not approve of is also proscribed.

The government has therefore taken steps to try to prevent use of the Internet for dissident organization and for accessing or disseminating information that it considers dangerous. Among other things this includes pornography, the ideas of the banned Falun Gong movement, and calls for the independence of Taiwan.

Recently, China has also turned its attention to spam. Because of the infrastructure put in place to monitor and filter Internet activity, the country may be in a good position to put effective spam controls in place.

Technology

The Chinese government has at its disposal all of the technology and know-how developed in the West for controlling and monitoring Internet traffic.

In November 2002, Amnesty International named 33 companies, including Microsoft, Sun, Nortel Networks and Cisco Systems, believed to be providing China with technology that it uses for Internet censorship. [Amnesty International, 2002] While a few companies denied that they were providing technology or services, others, including Microsoft and Cisco, basically said that the use made of the technology was not their concern.

However, individual Chinese who wish to get around the government’s censorship efforts also have technological allies in the West.

Filtering

Centralized control of all China’s border routers gives the government access to all traffic going to or from the Internet.

China’s government makes few public statements about its Internet filtering policies and techniques. To date, the best information on what is blocked and how comes from an ongoing study by researchers at Harvard Law School. By testing access to sites through Chinese Internet Service Providers (ISPs) and proxy sites, Jonathan Zittrain and Benjamin Edelman have been able to identify types of sites that tend to be blocked, and to draw inferences about the filtering technology in use.

Types of sites that are blocked

Sexually explicit sites are among those blocked by the Great Firewall, but Zittrain and Edelman found that well-known pornography sites were not blocked in China to nearly the same extent they are blocked in Saudi Arabia or by commercially available filtering applications such as those used in many American homes, schools and libraries. This suggests that blocking pornography is not a high priority for the Chinese authorities, despite its often being cited by the government as a type of content that is harmful to users.

Not surprisingly, political and news sites, particularly those having to do with Taiwan, Tibet, democracy in China and human rights, are among those that are frequently blocked. So are religious sites. Some more unexpected categories include health sites (particularly those dealing with famine in China, AIDS and mental health), education sites (including the Web pages of dozens of primary and secondary schools in the United States), and an eclectic assortment of entertainment sites.

Blocking technology

Zittrain and Edelman believe that “at least four distinct and independently operable methods of Internet filtering” were in use during the time of their primary study (May through November 2002), and that the government invests significant resources in

maintaining and refining its filtering systems, as well as updating the lists of blocked sites.

Types of filtering deduced by Zittrain and Edelman include:

- IP address blocking — This is believed to be the most common method in use. Very effective and efficient, as using China’s border routers to check the source IP addresses of packets against a list of blocked addresses is much faster and less processor-intensive than, for example, checking packet content for sensitive keywords. However, it is a rather crude method, resulting in blocking of an entire site (or even multiple sites that share a single host) even if only a small percentage of the content is objectionable.

- Keyword filtering of content — This is filtering of pages based on words or phrases that appear in the page content. While more sophisticated than IP blocking, content filtering requires analyzing the entire content of each packet and is thus very resource intensive. It seems to be used only sporadically and for certain targeted sites.

- Keyword filtering of URLs — This is filtering of pages and sites based on strings that appear in their URLs, particularly the names of political figures. This can result in the blocking of search results, as many search sites append search terms as part of the results page’s URL. It also allows blocking of cached pages on Google and other search engines that use “cache” as a URL parameter when a cached page is requested by the user. China also appears to use it to identify users searching for forbidden content, who may then have their Internet access entirely disabled for a period of time without explanation.

- DNS redirection — Chinese users who request pages from certain sites are sent to entirely different sites. The Domain Name Service (DNS) servers used to resolve domain names to their associated IP addresses apparently have been tweaked to report the IP address of an approved site when users attempt to access a banned site.

Spam

Recently, China’s government decided to take on spam (unsolicited bulk e-mail). In the West, its impact on productivity is usually seen as the largest problem with spam. In China, not surprisingly, the main concern is the content. The pornography and gambling marketed in many spam messages are illegal in China, and spam e-mails targeted at Chinese may also contain anti-government messages. [Associated Press]

In 2003, China began publishing lists of servers it believed were major sources of spam, and blocking them if they continued to send out spam. Most of the blacklisted servers are outside China. (Two-thirds of those on the first list were in Taiwan, a further indication that the government’s main concern is with political content.)

In addition to blocking known spam sources, the government is requiring the administrators of e-mail servers throughout China to take steps to prevent their being used as spam relays. [Lemon]

As these efforts are relatively recent, it is too soon to tell how effective they will be.

Viruses

Unfortunately, the Chinese government does not seem to have made filtering for viruses a priority, despite a recent study by the Ministry of Public Security that identified viruses as the largest threat to the security of China’s network.

Typically, viruses spread easily through China’s computer systems. The official figure on the percentage of computers infected with a virus during 2003 was 85%. The Sobig.F worm alone is believed to have infected 20 million computers throughout the country. [BBC News, 2003]

Some steps taken by the government may even have made the situation worse. In 2000, the *People’s Daily* described new regulations under which only the Ministry of Public Security would have the authority to confirm the existence of a virus and the efficacy of anti-virus software. One of the justifications the paper gave for the new rules was that they would “put an end to unfair competition among virus-killing software makers… [who] usually boasted of the omnipotence of their virus-killing software, or exaggerated the destructive potential of a virus.” [People’s Daily, 2000]

In addition to government inattention to the virus problem and distrust of “virus-killing software makers,” other contributing factors include the prevalence of pirated software (which, because it is not registered, can be harder to patch or upgrade) and simple lack of user awareness of the threat posed by viruses.

On February 11, 2004, Lu Chengzhao, deputy director-general of the Office of China National Network and Information Security Coordinating Group, announced that a National Network and Information Security System would be completed within five years. [People’s Daily, 2004] The announcement did not make it totally clear, however, whether the “emergencies” this system would be designed to respond to were specifically related to threats such as viruses, denial of service attacks and hacking, or whether it would handle incidents involving dissident communication as well.

Monitoring

Monitoring of Chinese Internet users’ activities is performed by both manual and automated means.

By the year 2005, all Internet cafés in China will be required to install surveillance software approved by the government that will immediately notify the authorities of any unauthorized Internet activity. [Amnesty International, 2004] In Shanghai, the government has installed video cameras as well. [BBC News, 2004]

China’s Ministry of Public Security (MPS) has hundreds of “computer supervision and monitoring units” throughout the country, particularly in major population centers [Hachigian], and 30,000 security personnel are believed to monitor Web sites, chat rooms and e-mail messages. [Boyd] In addition, ISPs and Internet Content Providers (ICPs), which are held accountable for what their users do online, often use their own monitors, known as “big mamas.”

Golden Shield

The “Golden Shield” is a project of the Ministry of Public Security, announced in late 2000. The goal of the project is to create a massive surveillance database accessible via a computer network linking national and local police agencies throughout the country. Little has been made public about the MPS’s progress in building and implementing the system.

Proactive Attacks

There may also be cases of Chinese authorities stopping information at the source, even when that source is outside the country. MPS personnel and other hackers working for the government are believed to have launched attacks that took Falun Gong and Taiwanese government Web sites offline. [Hachigian]

Circumvention

Chinese citizens wishing to get around the restrictions imposed by their government can often find a way to do so through trial and error. For example, content from blocked sites is often available through other sites that are not blocked.

In the most famous example, users in China were able for a time to get a wide variety of content via the search engine Google. Though links to pages returned in search results might be blocked, cached copies of these pages stored on Google’s servers were accessible until the government discovered this loophole and blocked Google in 2002. It was later unblocked when more sophisticated filtering allowed keyword-based blocking cached pages.

Though this use of their search tool was probably not intended by Google’s creators, other technologists in the West have deliberately set out to make it easier for dissidents and others in China to access blocked information.

Sites such as Anonymizer.com, known as “circumventors,” allow users to access sites blocked by their governments via a proxy server. Unfortunately, this only works if the government in question does not block the circumventor site, and China knows about and blocks all of the best-known ones.

(Interestingly, it was recently reported that under instruction from its backers in the U.S. government, Anonymizer.com censors what is available through the proxy by blocking sites with certain keywords in their URLs, including “hot,” “breast” and “gay.” Though intended only to block pornography, this crude filtering method results in many legitimate sites getting blocked. [McCullagh])

The difficulty of publicizing a circumventor to citizens of repressive regimes without alerting their governments to its existence has led to efforts for setting up large numbers of “grass roots” circumventors and spreading the word about them through personal contacts.

One example of this is the work of Bennett Haselton, a computer programmer and anti-censorship advocate commissioned by the U.S. government to produce an easy-to-use tool that allows Internet users around the world to set up their own circumventor sites. The software enables an individual to set up a small Web site that provides unfiltered access to the Internet through a Secure Sockets Layer (SSL) connection, and leaves no record of sites visited aside from the circumventor site. The circumventor site can be accessed and used by anyone who knows its URL, from dissidents in China to American teenagers whose parents have installed filtering software. [Festa, April 2003; Festa, May 2003]

Laws & Regulations

China has dozens of laws and regulations that pertain to the Internet. One reason for the proliferation of such laws is that many parts of China’s government are involved in regulating the Internet and issue separate laws on specific topics within their mandates. Some of the laws conflict with each other, and many are only selectively enforced, but others have a wide impact. [Hachigian]

Some of the major regulations include:

- Temporary Regulations Governing Computer Information Networks and the Internet (1996). These regulations established the government stranglehold over access to the Internet, requiring that “Any direct connection with the Internet must be channeled via international ports established and maintained by the Ministry of Post and Telecommunication. No group or individual may establish or utilized any other means to gain Internet access.” [Barmé & Sang]

- Telecommunications Regulations of the PRC (2000). These regulations outlaw the online transmission of “state secrets” and any information that jeopardizes national security, undermines national unity or social stability, disturbs the social order, etc., etc. Because the state can claim that almost any information it objects to falls into one of these catch-all categories, this law is one of the main justifications for the arrest of dissidents who use the Internet to communicate or publish information. The regulations also stipulate that operators of electronic bulletin boards and chat rooms must report “harmful” content, and that journalists and writers cannot post information until it has been approved by the government-controlled media.

- Measures for Managing Internet Information Services (2000). These regulate ISPs and ICPs, and require them to keep records on all of their subscribers.

- Additional regulations promulgated in 2002 increased the burden on Internet-related businesses. Among other things, the rules require ISPs to record messages and

report any illegal message content, and Internet cafés to install filtering software. They also make it illegal for anyone under 18 to enter an Internet café.

User & Industry Cooperation

The effectiveness of virtually all laws and policies is heavily reliant on the cooperation of those who are subject to them. China’s laws controlling Internet use are no exception.

Individuals

A company in America or the UK may have policies that forbid employees to take sensitive information home on a laptop or a diskette, but unless the company is a defense contractor or is in another highly sensitive and/or regulated industry, the physical and technological controls to prevent this happening are usually very limited or entirely absent. An employee with malicious intent would normally find it very easy to remove proprietary information from company premises. Even when there are technological controls in place, a knowledgeable and determined person can often find a way to circumvent them. It is the goodwill of employees and their willing adherence to company policy that actually keeps the information off the street.

Similarly, despite the technological controls described earlier in this paper, it is relatively easy for a Chinese citizen with Internet access to access forbidden sites, either through various circumvention techniques or simply because there is so much content on the Web that the government can’t effectively block it all. Yet there is little evidence that most Chinese do so.

“[T]he self-censorship that the regime promotes among individuals and domestic Internet content providers (ICPs) is the primary way officials control what Chinese viewers see.” [Hachigian]

Amnesty International believes that “Internet activism is continuing to grow in China as fast as the controls are tightened.” [Amnesty International, 2004] While this may be true, the majority of Chinese Internet users, and Chinese citizens in general, are more interested in economic issues than in politics. [Hachigian] They enjoy using the Internet to play games, communicate, and obtain what information is legally available to them, but have no wish to risk drawing the attention of the authorities by trying to circumvent government controls.

Industry

ISPs and ISCs (Internet Content Providers) in China are responsible for what their users do. A report from the Committee to Protect Journalists states that regulations controlling the content on Chinese sites, including news sites and Internet chatrooms, “turn Internet service and content providers into de facto government spies.” [IFEX] Similarly, laws require Internet cafés to police their users.

Companies that don’t cooperate face stiff penalties, typically including cancellation of the licenses they need to operate. This gives them a very strong incentive to go along with the government.

And it’s not only Chinese companies that are lining up to cooperate. Western companies such as American Internet giant Yahoo! voluntarily comply with restrictions on Web content in China in order to continue to have access to the market. [Hu]

Education

If a person believes that a rule is arbitrary or wrong or just not very important, that person may be less likely to make an effort to comply with it.

The Chinese are given little chance to deceive themselves that the government doesn’t consider control of the Internet to be extremely important. Setting up Internet access requires filling out a variety of official forms and pledging to use the Internet responsibly, so as not to threaten state security or reveal state secrets. The red tape for ISPs, content providers and Internet cafés also lets China’s Internet industry know exactly what is expected of them.

Chinese individuals and businesses are also very aware of the serious consequences of being caught breaking the rules.

But do the Chinese people agree with the government’s reasoning? Certainly there are many people who spout the party line, such as one Internet café manager who told an interviewer, “Absolute freedom is an impossibility. It would create anarchy. To censor harmful things…[will] ensure stability for China.” [Barmé & Sang] And according to Internet researcher Bobson Wong, “There have been surveys done of internet users in China, and the surveys reveal that most internet users in China trust the government.” [Boyd]

However, in a culture in which everyone is accustomed to carefully watching what they say, especially to the press, the true level of acceptance of Internet restrictions is very hard to gauge.

Enforcement

According to Amnesty International, as Internet use has increased in China, so has the number of people arrested for Internet-related activities. In early 2004, the human-rights watchdog group reported that at least 54 individuals were known to have been “detained or imprisoned for disseminating their beliefs or information through the Internet.” Roughly 100 more were believed to have been detained for spreading “rumors” about Severe Acute Respiratory Syndrome (SARS) via either the Internet or cellphone-based text messaging.

Prison sentences can be long, and treatment harsh. Several Falun Gong practitioners arrested for Internet-related offences have died in custody, possibly as a result of torture. [Amnesty International, 2004]

Enforcement of controls on Internet-related businesses can be equally harsh. In China, operators of e-mail services, newsgroups and chat rooms are liable for any security breach that occurs through use of their services.

In February 2000, the government shut down 127 Internet cafes in Shanghai because they had failed to obtain licenses. All of their computers were confiscated. [Getzlaff] In 2002, a fire at an Internet café in Beijing killed 25 people. The government responded by further crackdowns and more regulation on Internet cafés in Beijing and other cities. Apparently still unsatisfied with their level of control, the government has since announced plans to consolidate management of all of the country’s Internet cafés under about 100 sate-owned companies. [Lee]

China has also shut down entire sites because of content posted by individual users. In March 2004, Blogbus.com, which hosted blogs for more than 15,000 individuals, was taken offline because of the posting of a letter “critical of the government.” [Bodeen]

Such actions, combined with the strict licensing requirements, can leave Internet-related businesses in China with little sense that the government will grant them any leeway or leniency. In the interests of their own survival, most companies are probably quite diligent in following the regulations that require them to track and monitor their customers.

Other Countries with Nationwide Internet Controls

Though China is perhaps the best-known example of a country that keeps close tabs on Internet usage, it is far from being the only one. Countries known or believed to perform extensive filtering of online content include Singapore, Cuba, Saudi Arabia, Iran, Vietnam, Syria and many others. A few of these are briefly discussed below.

Singapore

This tiny but heavily wired nation in many ways has served as China’s model for Internet control. The Singapore Broadcasting Authority (SBA) requires that all Internet traffic pass through routers controlled by the government, requires content providers to be licensed, and instructs ISPs to block sites whose content “undermines public security, national defence, racial and religious harmony and public morality.” Singapore has also set up a task force to educate citizens on appropriate online behavior. [Reporters Without Borders; Singapore]

Saudi Arabia

Saudi Arabia performs extensive filtering, but with some interesting differences from China.

Despite being a society in which free speech is not a right and expression of dissident political and religious beliefs is not tolerated, Saudi Arabia does not censor nearly as many sites as does China. Pornography is much more thoroughly filtered than in China, along with sites dealing with sexuality in general and sites providing information specifically to and about women. However, sites dealing with political and religious issues are only selectively blocked, and news sites, U.S. government sites and education sites are generally available.

Saudi Arabia is also more open than China about its filtering operations, starting with being very up front about the fact that the government blocks access to nearly 400,000 Web pages. [Reporters without Borders, 2004] When a Saudi tries to access a blocked Web page, a message appears informing him or her that the page has been blocked. In China, when a page does not appear it is often hard to tell whether this is due to blocking or to a technical glitch. [Zittrain & Edelman, 2002]

The Saudi authorities have even been known to unblock sites upon request. In 2004, they unblocked two gay Web-sites after verifying that they contained no pornographic content, despite the fact that homosexuality is illegal in Saudi Arabia. [Reporters without Borders, 2004]

The United States

In the United States, any attempts to control or monitor Internet usage must be handled either covertly or very carefully in order to avoid an outcry from free-speech and privacy advocates. However, it is widely believed that the National Security Agency (NSA) routinely monitors Internet traffic and phone calls for signs of criminal and terrorist activity. Because many foreign communications pass through U.S. systems, they are monitored as well.

The NSA is very close-mouthed about such monitoring. However, in early 2004 a message intercepted by NSA intelligence officers launched investigations that eventually led to the arrest of Canadian software developer Mohammed Momin Khawaja. [Akin]

Although the U.S. government published the *National Strategy to Secure Cyberspace* in February 2003 [The White House], its provisions are merely guidelines and recommendations and there are no plans to enforce them.

Conclusion

Though China is more concerned with protecting against ideas than protecting against viruses, hacking, data theft and other typical information-security issues, its techniques for controlling the Internet have much in common with information security strategies used in countries and corporations around the world.

Government/management support. China’s broad control of the Internet within its borders would not have been possible without the strong support of the central government. Where this support has been lacking — for example, in the case of virus protection — there is a noticeable lack of effective action. Similarly, security initiatives in other countries and in corporate environments require strong support from high-level leadership, to ensure that they receive the necessary publicity and resources.

Filtering. Though China controls all of its border routers and has made a significant investment in filtering technology, it still runs into the same issues as companies, libraries, schools and parents who want to provide Internet access yet filter pornography, hate speech or other content:

- Site blocking is only partly effective, because it’s impossible to keep up with all of the sites and pages that are available. It also leads to over-blocking, where sites and pages with innocuous content are blocked along with those deemed objectionable.

- Keyword blocking is slow and expensive, can be tricked by coded language (whether it’s “V1@gr@” or “T@1w@n”), and also can lead to blocking of inoffensive content.

- No matter how good the technology is, users who are motivated to will usually find a way around it.

Monitoring. With sufficient human and technological resources, monitoring can be pretty effective. In a free and open society, however, heavy-handed monitoring is likely to engender a lot of opposition and may even be illegal in some cases. Democracies must be very circumspect in monitoring the online activities of their citizens, while corporations have more leeway to monitor activity on their networks.

Balance. China must balance the needs of business with the government’s need to control information. Too much filtering can overload the system, slowing down traffic. Restricting encryption or being too obvious about monitoring traffic leads to a risk or losing business from countries, such as those in the EU, that require strict controls on the privacy of personal information.

Similarly, corporations must balance the need for fast and easy access to information with the need for adequate information security.

Rules. Laws and policies are critical, as they make desired standards of behavior enforceable. But if those who are subject to them either don’t agree with them or see little consequence to noncompliance, they aren’t likely to achieve the desired results.

Education and enforcement. The key to information security, whatever your definition of it, is making it clear to users, system administrators, business owners and others what is expected of them, and providing prominent examples of consequences for breaking the rules.

Obviously, this does not mean that corporate employees who take proprietary data home on a laptop or forget to install a security patch on a server should be thrown in prison and tortured. But no information security strategy can succeed without clear rules, an awareness campaign to ensure that all those who are involved understand the rules and why they were put in place, and consistent and public enforcement.

List of References

Akin, David. “Arrests key win for NSA hackers.” Globe and Mail Update. Tuesday, April 6, 2004. URL: http://www.globetechnology.com/servlet/story/RTGAM.20040406.gtterror06/BNStory/Technology/ (April 8, 2004)

Amnesty International. “People’s Republic of China: State control of the Internet in China.” November 26, 2002. URL: http://web.amnesty.org/library/Index/engASA170072002 (February 24, 2004)

Amnesty International. “People’s Republic of China: Controls tighten as Internet activism grows.” January 28, 2004. URL: http://web.amnesty.org/library/index/engasa170012004

Associated Press. “China vows to curb junk e-mail.” SiliconValley.com. February 2, 2004. URL: http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7855530.htm (February 11, 2004)

Barmé, Geremie R., and Sang Ye. “The Great Firewall of China.” *Wired*. Issue 5.06; June 1997. URL: http://www.wired.com/wired/5.06/china_pr.html (February 24, 2004)

BBC News. “Computer viruses rampant in China.” October 21, 2003. URL: http://news.bbc.co.uk/1/hi/technology/3210086.stm (May 7, 2004)

BBC News. “Shanghai cameras spy on Web users.” April 22, 2004. URL: http://news.bbc.co.uk/2/hi/asia-pacific/3648813.stm (May 9, 2004)

Bodeen, Christopher. “Group: China shuts down Internet blogs.” Salon.com. March 19, 2004. URL: http://www.salon.com/news/wire/2004/03/19/blogs2/print.html (March 19, 2004)

Boyd, Clark. “Bypassing China’s net firewall.” BBC News. March 10, 2004. URL: http://news.bbc.co.uk/1/hi/technology/3548035.stm (April 13, 2004)

Festa, Paul. “Cracking the great firewall of China.” CNET News.com. May 20, 2003. URL: http://news.com.com/2102-1082_3-1007974.html (February 24, 2004)

Festa, Paul. “Software rams great firewall of China.” CNET News.com. April 16, 2003. URL: http://news.com.com/2100-1028-997101.html (February 24, 2004)

Getzlaff, J.A. “The Great Firewall of China.” Salon.com. February 22, 2000. URL: http://dir.salon.com/travel/planet/2000/02/22/shanghai/index.html (February 24, 2004)

Hachigian, Nina. “China’s cyber-strategy.” *Foreign Affairs*. Vol. 80, no. 2; March/April 2001. URL: http://www.rand.org/nsrd/capp/cyberstrategy.html (February 24, 2004)

Hu, Jim. “Yahoo yields to Chinese web laws.” CNET News.com. August 13, 2002. URL: http://news.com.com/2100-1023-949643.html?tag=nl (May 7, 2004)

IFEX (International Freedom of Expression eXchange). “CPJ examines the great firewall of China.” Vol. 10, no 3; January 23, 2001. URL: http://www.ifex.org/en/content/view/full/28000/ (February 24, 2004)

Knight, Will. “Google mirror beats Great Firewall of China.” NewScientist.com. September 6, 2002. URL: http://www.newscientist.com/news/print.jsp?id+ns99992768 (February 24, 2004)

Lee, Zen. “China clamps down on Internet cafes to protect ‘mental health.’” CNETAsia. March 25, 2004. URL: http://news.zdnet.co.uk/internet/security/0,390203075,39149878,00.htm (March 31, 2004)

Lemon, Sumner. “China upgrades antispam efforts.” IDG News Service. February 20, 2004. URL: http://www.pcworld.com/news/article/0,aid,114867,00.asp (February 24, 2004)

McCullagh, Declan. “U.S. blunders with keyword blacklist.” CNET News.com. URL: May 3, 2004. http://zdnet.com.com/2100-1107_2-5204637.html (May 6, 2004)

People’s Daily Online. “China issues new rules on fighting computer viruses.” May 27, 2000. URL: http://fpeng.peopledaily.com.cn/200005/27/eng20000527_41735.html (May 7, 2004)

People’s Daily Online. “China to complete national network and information security system in 5 years.” February 13, 2004. URL: http://fpeng.peopledaily.com.cn/200402/13/print20040213_134785.html (February 19, 2004)

Reporters without Borders. “Ban lifted on two gay websites.” March 30, 2004. URL: http://www.rsf.org/article.php3?id_article=9586 (May 3, 2004)

Reporters Without Borders. “Singapore.” URL: http://www.rsf.org/article.php3?id_article=7247 (May 3, 2004)

Richardson, Tim. “Outcry as Chinese Net dissident arrested.” The Register. February 17, 2004. URL: http://www.theregister.co.uk/content/6/35619.html (February 19, 2004)

Thorsell, Staffan. “The Great Firewall of China.” Guardian Unlimited. April 24, 2003. URL: http://www.guardian.co.uk/china/story/0,7369,942954,00.html (February 24, 2004)

The White House. The National Strategy to Secure Cyberspace. February 2003. URL: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Zittrain, Jonathan, and Benjamin Edelman. “Documentation of Internet filtering in Saudi Arabia.” Berkman Center for Internet & Society, Harvard Law School. September 12, 2002 update. URL: http://cyber.law.harvard.edu/filtering/saudiarabia/ (May 3, 2004)

Zittrain, Jonathan, and Benjamin Edelman. “Empirical analysis of Internet filtering in China.” Berkman Center for Internet & Society, Harvard Law School. March 20, 2003 update. URL: http://cyber.law.harvard.edu/filtering/china/ (February 24, 2004)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS