White Paper

Defeat Internet Censorship: Overview of Advanced Technologies and Products

Global Internet Freedom Consortium (GIFC)
http://www.internetfreedom.org/
contact@internetfreedom.org

November 21, 2007

TABLE OF CONTENTS

1 Introduction

The Internet has become a revolutionary force in repressive regimes. The free flow of information and idea exchange has been perceived as a threat, rather than a blessing, by the authorities in these countries. In response, they have imposed strong censorship on Internet usage by monitoring, filtering, tracing and blocking data flows, using advanced technologies. Confined to a tailored and distorted cyberspace, innocent citizens face constant threats when they read, write or speak on the Internet, as their privacy is exposed under the authorities' watchful eyes. The consequences can be life-threatening. In this environment, the service and content providers practice a great deal of self-censorship[1].

Since late 1990s, there have been heroic efforts from grassroots organizations to defeat the censorship, with technological counter-measures. These efforts are mostly in the form of computer and Internet technologies to evade data monitoring, circumvent data flow blocking, or defeat tracing. These technologies vary greatly from each other in their objectives, designs and implementations, and have significantly different strengths and weaknesses.

In addition, they have wide range of maturity levels and life-cycles. Some have been field-proven and in operation for many years. Some have always been in design and development mode since day one. Some stirred up quite some media hype initially but never materialized. Yet, some have been quietly and persistently running in semi-underground mode for many years with great achievements.

This article aims to provide a non-technical overview of the leading and most influential technologies used to circumvent Internet censorship in repressive regimes. We will also discuss the software packages that were found to be most effective in countering the blockage for end-users. Thus, this article will document the state of the art in this field, and provide practical guidance for users who need to make judicious choices of the best tools available for their protection.

We will use the censorship in China as the primary example because the most advanced censorship technologies have been deployed and tested there. The circumvention tools to defeat the censorship in China will work equally well or better in other countries.

2 Censorship Tools and Methods

Internet censorship refers to technical and non-technical measures taken by repressive regimes to limit a user's freedom to access information on the Internet. Such measures include, but are not limited to: monitoring of users Internet activities, denying users access to certain websites (blocking), tracking and filtering users' data flow, and disciplining website operators to tailor

[1] Human Rights Watch, 2006: Race to the Bottom: Corporate Complicity in Chinese Internet Censorship. *Human Rights Watch*, Vol. **18**, No. 8C.

their content to comply with censorship regulations. Sometimes the Internet censorship is also referred to as Internet blocking or jamming.

Internet censorship circumvention refers to counter-measures to Internet censorship, with emphasis on technical means to protect users in repressive regimes from being monitored, blocked or tracked, and to provide users with as much freedom of access to information on the Internet as in the free countries. Such measures are also called "anti-blocking" or "anti-jamming" among some of the circumvention developers.

To implement Internet censorship, China has imported the most advanced networking technologies and equipment from western countries, to build the "Chinese Great Firewall" (GFW). Currently the most critical components are implemented on their international gateway, to perform three fundamental functions of Internet censorship:

- IP-address blocking. The GFW maintains a blacklist of IP addresses, most of which are websites or other services they do not want users to access. The blacklist is manually updated based on demand of their blocking needs[2].
- DNS hijacking. This malicious mechanism can redirect a clueless user to a totally different website from what he intended to view, by snooping the user's domain name resolution (DNS) request and supplying the user with a false reply. Currently many of the blocked websites (e.g., the Voice of America website, www.voa.gov) are done this way.
- TCP content filtering. Most Internet traffic is carried in truckloads called TCP segments. Their firewalls constantly capture and analyze the content of every user's Internet TCP segments, and will cut off their two-way Internet communication once the firewall matches any pre-defined signatures, such as sensitive keywords, especially in Chinese (e.g., "Falun Gong")[1] .

These three mechanisms are the building blocks of the Great Firewall's foundation. Any censorship circumvention technique must evade or defeat them by design for long-term success.

The censors' blocking targets fall into two categories: websites and circumvention tools. Conventional websites are sitting ducks[3]; they can easily be blocked by IP addresses blocking or DNS hijacking. Nowadays, the full suite of blocking measures are firing at circumvention tools by identifying the location and traffic patterns of the circumvention tunnels these tools tend to use.

The censors do not apply these blocking mechanisms blindly. They methodologically aim at the biggest targets on their radar screen, and focus their resources on them first. For example, Garden, UltraSurf and DynaWeb have been heavily blocked by Chinese censors, because they have the biggest user bases and best service coverage. Other newer tools, such as Tor, GPass and FirePhoenix, have not stood out enough to attract focused blocking.

[2] Chase, M. S. & J. C. Mulvenon, 2002: You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies. RAND, 132pp.
[3] Zittrain, J. & B. Edelman, Empirical analysis of Internet filtering in China. http://cyber.law.harvard.edu/filtering/china/

Besides these censoring controls through technological approaches, we want to note another form of censorship, namely, self-censorship by content providers or websites operators. International companies doing business in censorship countries, such as China, restrict themselves and provide tailored content to users in these regimes. A prime example is Google's Chinese version, which provides drastically different search results for queries originating in China from its versions in other locations[4]. A side-by-side comparison in real-time between Google's Chinese and overseas version[5] reveals the Chinese version to be highly censored, partial, biased and misleading. Unfortunately, there exist no effective technical measures to defeat such a form of censorship.

3 Brief History of Internet Censorship and Circumvention

The Internet censorship and its circumvention technologies did not reach the current state of sophistication in one day. The evolution of the field has been driven by a long, dynamic, and invisible battle between the two sides.

The earliest form of Internet censorship was IP-address blocking in China in the late 1990s. As the usage of Internet expands from academia to the mass, and many traditional media established Internet presence, the communist authorities quickly realized the threat of information infiltration and implemented the rudimentary form of blocking. They transferred their blacklist in radio and television jamming to the Internet domain, and users found they could not access websites such as Voice of America (VOA) or Radio Free Asia (RFA). However, unlike radio or television jamming about which users cannot do much, tech-savvy users on the Internet found ways to circumvent. A cat-and-mouse game started.

Most of the circumvention techniques at that time relied upon open web proxy servers, or proxies. These proxies are websites which can fetch pages from blocked websites and pass them to users, working much the same way as the Underground Railroad in the 1800s. Many overseas volunteers, many of whom would later become developers of various circumvention tools, regularly collected open proxies and posted them to websites to facilitate users inside China.

The period from 2000 to 2002 saw a dramatic escalation of China's blocking technology and intensity. Two advanced technologies, secretly implemented, caught many of the anti-blocking experts off guard: one was the dynamic filtering of Internet data flow, and the other was the DNS hijacking mechanism[6]. These two new measures made it impossible to use proxies alone to penetrate the Great Fire Wall. A few elite underground groups quickly figured out the workings of these two measures, and developed various counter-measures, which later would lead to some of the most popular anti-blocking software systems today. Meanwhile, totally unaware of the tricky blocking situation, some high-profile hacker groups proposed new ideas beyond the proxies approach and some provided prototype implementations. Unfortunately,

[4] DIT Inc., 2006: Report on Google.cn's Self Censorship. http://back.dit-inc.us/report/googlecn_report.html
[5] http://www.williamsburger.com/google/
[6] DIT Inc., 2002: Forbidden sites hijacked all over China. http://www.dit-inc.us/report/hj.htm

most of them did not turn into easy-to-use products for average, foreign language-speaking users. But their ideas were later absorbed into some of the successful products.

The battle between the two sides has been very dynamic. The GFW technologies kept improving, in an attempt to defeat the ever popular circumvention systems. However, the anti-blocking experts worked hard to counter the censors. Today, in this engaging battle, a few of the circumvention tools have clearly gained the upper hand; they are supporting a large number of users, have become household names in China as well as big targets on GFW's radar screen. Theoretically, it is still possible for the censors to block these tools[7], but they have to work much harder nowadays as the anti-censorship tools are technically more sophisticated. Moreover, censors have to think twice before deploying new blocking technologies, because if such technologies are not well enough tested, they can be tricked by contenders to block unintended sites or even themselves, as happened before at their early stage of DNS hijacking implementation[8].

However, there is one frontline of the battle that has been ignored until now by the anti-censorship community. Besides technological pursuit in censorship implementation, the Chinese communist regime makes strategic plans to export their propaganda and disinformation machinery to free countries inconspicuously, apparently, applying the "an offense is the best defense" philosophy. Many Chinese-language websites, as well as newspapers in the United States are largely controlled by Beijing through ways such as investment or joint venture, and these media can spread the same disinformation in the western world as on the other side of the GFW[9]. Sometimes it is ironic to see web surfers from China, after successfully penetrating the GFW, end up in traps skillfully set up by the censors they are trying hard to evade. Hereby it is important to build and maintain trustworthy content platforms in their native language, to provide users with a true, independent cyberspace immune to the censors' infiltration.

4 Anatomy of an Anti-Censorship System

The ultimate function of an anti-censorship system is to connect censored users to uncensored Internet securely and anonymously. This function requires a complex system with many components working together. Figure 1 shows the components of a typical anti-censorship system. Censored users (1) use circumvention client software (2) on their computers to connect to circumvention tunnels (4), usually with the help of a tunnel discovery agent (3). Once

[7] Haselton, B., 2006: Behind the Magic of Anti-Censorship Software. http://yro.slashdot.org/yro/06/12/20/1336245.shtml

[8] When GFW first deployed the DNS hijacking mechanism, Dynamic Internet Technologies (DIT), registered domain names such as "nhuanet.com". Chinese censors quickly put such a domain name in the DNS hijacking's keyword list, inadvertently tricked GFW into hijacking the domain name of their own propaganda backbone site, "xinhuanet.com", which contains the keyword registered by DIT. They later refined their keyword matching algorithm in GFW.

[9] The Epoch Times, 2006: The Chinese Communist Regime's Control of Overseas Media: Interview with Ms. He Qinglian. http://en.epochtimes.com/news/6-8-18/45088.html

connected to a circumvention tunnel, a user's network traffic will be encrypted by the tunnels and penetrate the GFW (7) without being detected by the censors (6). On the other side of the GFW, the network traffic will enter a circumvention support network (8) set up and operated by anti-censorship supporters (9). The computers, sometimes called nodes, in the circumvention support network act as proxies to access content from the unobstructed Internet (10) and send the information back, not necessarily taking the same route, to the censored user's computer.

Initially if a censored user knows nothing about the other side of the GFW, it is necessary to get them bootstrapped by employing out-of-band communication channels (5). Such channels include emails, telephone calls, instant messages, and mailing of CD-ROMs. Sometime users can also take advantage of these channels to locate circumvention tunnels (4), if the client software in use does not have a tunnel discovery agent (3).

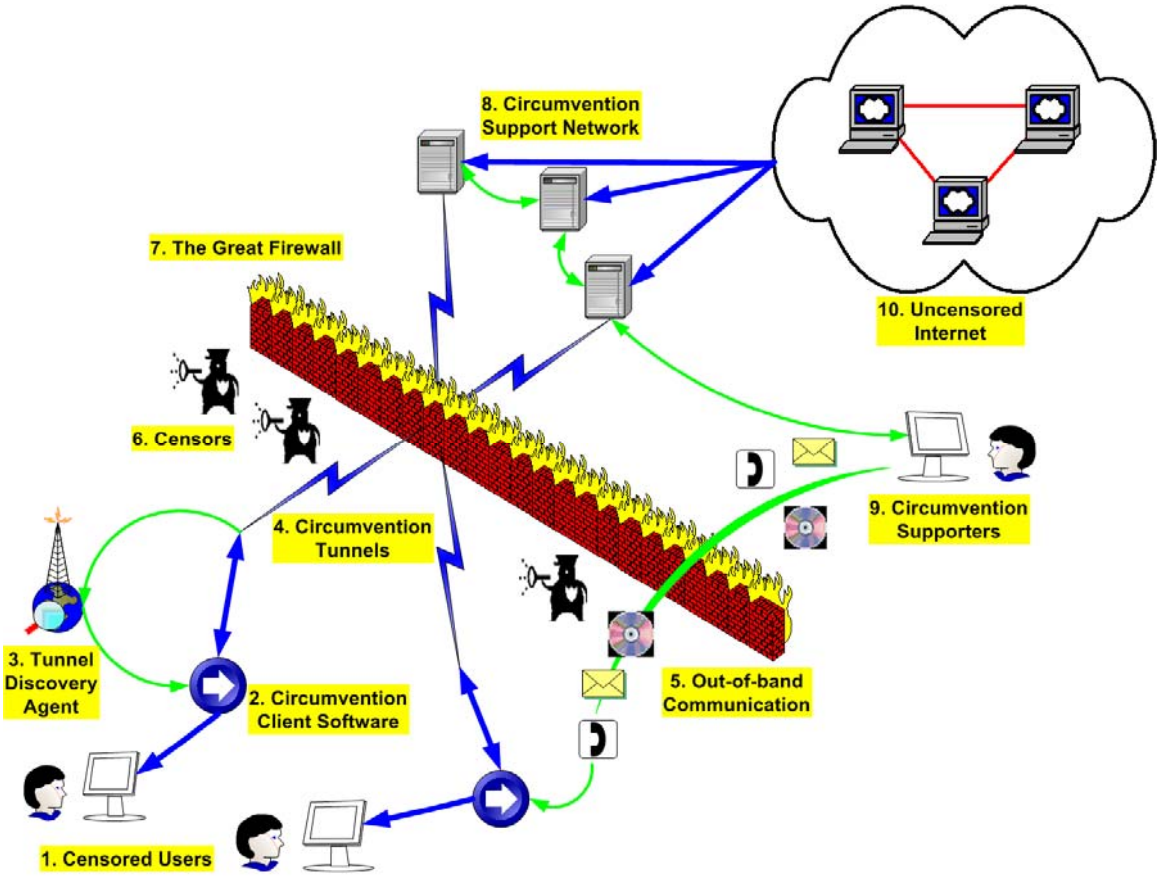

Figure 1. Anatomy of anti-censorship system.

In fact, the most mysterious component in an anti-censorship system is the tunnel discovery agent (3). With such an agent, a user does not need to configure the software. The agent will automatically find circumvention tunnels for the user's particular client software. Little public information is available from the most successful anti-censorship tools, because their technologies are proprietary and source code is not available. Some of the agent

implementations may have exploited weaknesses in the GFW technologies and can blend the discovery traffic with regular traffic without being detected. The continual success of the leading anti-censorship tools (Garden, UltraSurf and DynaWeb, Sec. 6) for so many years can be significantly attributed to their innovative tunnel discovery agent designs.

5 Anti-censorship Technology Categories

There are many conflicting requirements for an anti-censorship system. Each existing tool has evolved through a practical balancing between these requirements.

5.1 Client Software or No Client Software

There are two ways of anti-censorship support that the technology evolved. At the early stages, when censorship penetration mainly relied on open web proxies, a user did not need to install any additional software. He/she just collected the addresses of the proxies, and took advantage of most web browser's built-in support of proxies to circumvent blocking.

As the blocking intensified, it became harder to find usable proxies. Even worse, after content filtering was implemented in GFW, information flow through proxies could be intercepted by GFW since most proxies did not support encryption. A natural step is to provide users with special software which has functions similar to proxies, but with the flexibility to build in customized encryption, friendly user interface, native language support and many other features. Nowadays, most anti-censorship approaches depend on special software packages. However, they come with the extra effort of sending the software to the users.

The software-based anti-censorship provides users with much freedom. Newer software systems can not only support unobstructed web surfing, but also provide security and anonymity for communications with other Internet protocols, such as emails, various instant messaging (IM) systems, and multi-media streaming.

5.2 Green or Non-Green

Chinese users have coined the term "green software" to refer to software that does not need an installation process. Ideally such software is a single, executable file which can run on any Windows computer. This is an important factor in determining the popularity of the software. Users in censored territories have a different Internet environment than what we are accustomed over here. For example, in China, a large fraction of Internet users go to Internet cafés for their surfing. Typically, the computers there either do not allow users to install software, or they are wiped clean periodically. Thus, it would be of great convenience if users can store the software on a USB flash drive or a CDROM, and use the software wherever they go.

Of course, being "green" imposes some limitations on software's capability. It is impossible to implement some advanced features with green software.

5.3 Mouse or Tiger

Within the anti-censorship community, there are two schools of philosophy. One might be called the "Mouse's way", and the other, the "Tiger's way." The Mouse's way is a strategy to keep a low profile, make the user base small, and pass along the software based on personal trust. The hope is that the effort will not become a target on the censor's radar screen, and the software won't fall into the hands of the adversary for possible cracking.

By contrast, the Tiger's way is more open. Such an approach tries to reach as many users as possible by mass mailing, messaging and word-of-mouth. The software is posted on many websites for users to freely download. Open forums are made available for users to post feedbacks and exchange experiences.

The Tiger's way provides better protection for every user, though it appears as a big target on the censor's radar screen. With a large enough user base, the network activities from any particular type of user (such as political dissidents) blend in the background well and it is impossible for the authorities to single them out. However, Tiger-grade anti-censorship software has to be well built to resist cracking, reverse-engineering and modification when fallen into an adversary's hand. The Mouse's way, on the other hand, faces the constant threat that once the software's traffic pattern is recognized, the small user base can be easily isolated and identified.

5.4 Open Source or Proprietary

The software packages of various anti-censorship tools also fall into two categories: open-source and proprietary. Open-source software follows the tradition of the general open source community, and the release of such software together includes the source code. This facilitates community participation and scrutiny, but meanwhile totally reveals the inner working of the system to adversaries.

Proprietary software has the advantage of hiding a great deal of the software's working, with the help of techniques such as code obfustication, code signing, wrapping and even using decoys. More importantly, a few of the leading proprietary systems, apparently, pack some unconventional techniques to exploit unpublished weakness of censorship systems, especially the GFW, in a way similar to the zero-day exploits hackers use. It is obviously a disadvantage to release the source code of such a system to the public. So some groups have understandably treated their source code similar to a trade secret.

5.5 Content Control or No Control

Ironically, to provide better anti-censorship service, the service operators may need to impose some form of control and limit on the content they provide. That is because an anti-censorship tool does not only provide users in oppressive regimes access to censured content, it may also be used by users to access and distribute pornography and illegal contents. As a matter of fact, without content control, "unintended" content can easily overwhelm other information categories. For example, an estimate made in 2000 shows that 89% of the images hosted on

Freenet was pornography[10]. With limited resource and bandwidth, an anti-censorship system with unrestricted access will soon be consumed by pornography, gambling and drug-related information and become useless to users in the most needed regions. Therefore, it is critical and beneficial for an anti-censorship system to have some built-in mechanisms to control content access. At least, it should have the ability to block some high-profile pornography portals in order to save the bandwidth for better uses. It should also provide tools for law-enforcing authorities in the free world to monitor the information flow when needed to avoid the encryption channels being exploited for terrorist communications.

5.6 Anonymization vs. Anti-Censorship

There is a type service available on the Internet, called anonymization, which can masquerade a user's IP address when he/she surfs the web, and encrypt the user's traffic. This service, mostly paid, shares some functionality with anti-censorship tools. However, it cannot be used as a circumvention tool in countries like China, as it lacks the necessary sophistication such as anti-DNS-hijacking, node discovery, etc. Hence, this service is rendered vulnerable and can be easily blocked in China. For users in net-policing countries, this service is not recommended.

6 Anti-Censorship Technology Overview

In this section, we examine influential censorship circumvention technologies developed since the late 1990s.

6.1 Freenet

Freenet was the brainchild of Ian Clarke in 1999[11]. It was designed to be a decentralized, peer-to-peer (P2P) network built atop the Internet, to support totally anonymous information publications, storage and retrieval. It has been under development since then, and has gone through numerous revisions. The current release is Freenet 0.7.

Freenet stands out as a potential anti-censorship system among other P2P systems, as it promised a drastically different P2P network with no central control. Most P2P systems, notably those popular file-sharing networks such as Napster and Gnutella, rely on a central directory service for peers to announce and locate other peers. Such architecture is vulnerable to attack by censors as they can easily block the central directory servers and cripple the whole system. Freenet avoids the usage of a central directory service. Instead, it relies on inter-node communication and referral to eventually find a document on the network. In addition, information on Freenet is not stored on fixed computers. It can migrate within the network depending on usage patterns. Therefore, it can achieve total anonymity for both content

[10] Orwant, J., 2000: What's on Freenet? http://www.openp2p.com/pub/a/p2p/2000/11/21/freenetcontent.html
[11] Clarke, I., 1999: A distributed decentralised information storage and retrieval system. http://freenetproject.org/papers/ddisrs.pdf

publishers and readers, and the decentralized P2P architecture defies blocking by censors, especially when the number of Freenet nodes is large.

At the early stage, many groups in the anti-censorship community were hopeful that Freenet would be the ultimate weapon to defeat Internet censorship. A group even put up a Chinese website promoting Freenet[12]. However, so far Freenet's usability and performance have not been satisfactory, and it has not achieved explosive growth in its user base. In particular, like a separate plumbing system, Freenet does not interoperate with the rich content on the World Wide Web. A user must use Freenet's publishing system to feed content into the network. Due to these limitations, we do not expect Freenet to play a major role in the battle against censorship anytime soon. Its market share will not experience notable growth without active promotion and user support.

6.2 Triangle Boy

Originally developed by Safeweb (www.safeweb.com) and officially launched in October 2000, Triangle Boy received a lot of media attention in early 2001, when CIA's venture capital company, In-Q-Tel, decided to invest in this technology. It was deployed and used in countries such as Saudi Arabia and China on a limited scale. China succeeded in blocking Safeweb's in March 2001[13]. Largely due to the lack of dedicated operational efforts, Triangle Boy did not catch on, and in 2003 Safeweb was acquired by Symantec, which apparently did not have any interest in supporting Triangle Boy and its censorship circumvention operation.

Despite of its short life span, Triangle Boy left a long-lasting imprint in the anti-blocking technology arena. Its main idea is as follows. First, Safeweb provides servers that function like web proxies to fetch web pages for its users; however, users do not connect directly to Safeweb's proxy servers, which are susceptible to blocking like regular web proxies. Instead, users first connect to third party computers, called nodes, which run the Triangle Boy software and forward users' requests to Safeweb's proxy servers. The Safeweb's servers then return the traffic directly to the users, masquerading the returning traffic as if from the nodes. From a censor's perspective, the users are interacting only with the nodes. Hence, Safeweb's servers are invisible to a censor.

Theoretically, if one can find enough volunteers to run a large number of nodes with dynamic IP addresses, it would be extremely hard for a censor to block them all. But it is this very operational aspect of finding volunteers to support enough nodes that proved to be harder than developing the technology, and it is one of the primary reasons Triangle Boy failed to reach critical mass.

At the time of Triangle Boy's debut, the censorship technologies had not grown to their full sophistication yet. Therefore, Triangle Boy's design goal was only to defeat IP-blocking. It would not work at later times when DNS-hijacking and content filtering were in place. Nevertheless, Triangle Boy served well as the first working instance of using nodes to deflect Internet traffic and to defeat IP-blocking.

[12] http://freenet-china.org/
[13] http://censorware.net/article.pl?sid=01/03/14/0755209

6.3 Garden

Garden is one of the earliest smart proxy systems, first launched in 2001 by Garden Networks (www.gardennetworks.com). It has been one of the most popular anti-censorship systems in China, and together with UltraSurf and DynaWeb (see below), it has been called, affectionately, one of the three anti-blocking "swordsmen" by Chinese Internet users. It has been actively improved and supported by a dedicated team of volunteers. The current version is Garden 3.5.

Garden was built upon the simple web proxy idea with a small piece of client software running on a user's computer. The client software does smart things to improve both the security and usability of the anti-censorship functionality. It dynamically locates overseas Garden proxy servers to avoid IP blocking, encrypts users' traffic to evade content filtering, and employs URL-rewriting technology to defeat DNS-hijacking. In addition, Garden software can clean up users browsing history on their PC for enhanced security. These functions are performed automatically without user intervention, so it suits non-technically savvy users well. Apparently, Garden keeps a large pool of well maintained proxy servers overseas with content caching, which greatly improves user experience.

Garden's technologies have defeated GFW's censorship well. Though Garden has been on top of GFW's target list and has attracted a large number of users, the Chinese Communists have not been able to stop the information flow through GFW via Garden's pipes. Garden's success, especially in China, is largely attributed to its usability and operational support. At its early stage, it had Chinese language support, and established its presence on an anti-censorship communication platform (www.qxbbs.org) by a dedicated support team. Later, Garden's technology and software became mature and stabilized. We recommend more operational support and resource expansion to make Garden still stronger.

6.4 UltraSurf

UltraSurf is the flagship anti-censorship product by UltraReach (www.ultrareach.com), an Internet technology company founded by a group of Silicon Valley technologists. Since 2002, UltraReach has focused its core business on developing anti-censorship technologies, and the current release of its anti-censorship software is UltraSurf 8.8. UltraReach has been expanding its offerings based on its unique GIFT (Global Internet Freedom Technology) platform, and today it is also providing a secure email service called UltraMail, and a protected web portal for users in China, UltraReach.net (or www.wujie.net). UltraSurf's Chinese name, Wujie – meaning borderless – has become a household name among Chinese Internet users. UltraSurf is one of the "three swordsmen," thanks partly to its user friendliness and user support in Chinese.

UltraSurf is a robust anti-censorship system evolved from the lasting battle between GFW and UltraReach. Since infancy, UltraSurf has been one of the Chinese Communists' favorite targets. The freely available software has been analyzed, mutilated and spoofed, and the supporting network infrastructure has been constantly attacked. Without doubt, these factors have accelerated UltraSurf reaching its level of sophistication and fame.

The current release, UltraSurf 8.8, has implemented a complex proxy system with complete transparency and a high level of encryption on the Microsoft Internet Explorer (IE) platform. UltraSurf 8.8 enables users to browse any website freely--just the same as using the regular IE browser--while it automatically searches the fastest proxy servers in the background. It has strong support for load balancing and fault tolerance, and it even employs a decoying mechanism to thwart any tracing effort of its communication with its infrastructure.

6.5 DynaWeb

DynaWeb is a collection of anti-censorship services provided by Dynamic Internet Technology Inc. (DIT). DIT was founded originally in 2001 to provide email delivery services to China for U.S. government agencies and NGOs. In 2002, DIT started to provide anti-censorship services under the framework of DynaWeb, and like UltraSurf, DynaWeb became a top contender of the GFW-penetration effort. The battle between DynaWeb and GFW has been thrilling, dynamic and dramatic, albeit largely invisible to the general public. Today DynaWeb offers the widest range of options for users to access Internet freely, and supports more than 50 million web hits per day on average from Chinese users alone.

DynaWeb is a web-based anti-censorship portal. Once users point their web browser at one of the DynaWeb URLs, a web page will be presented similar to the one at www.dongtaiwang.com, with most blocked websites as links. In addition, a user can type in any URL in the box on this page and DynaWeb will fetch the pages for him/her instantly. No software is needed, nor are any settings tweaked on a user's computer. But since the Chinese net police watch DynaWeb's portal websites closely and block them as soon as they identify them, DynaWeb must indeed be very dynamic. It has hundreds of mirror sites at anytime, and each with a varying IP and DNS domain name, to defeat IP blocking and DNS hijacking. On the backstage, DynaWeb also has mechanisms to proactively monitor the blocking status of each of its mirror sites, and as soon as blocking is detected, it will change the IP and DNS domain name instantly.

To keep users connected to such a dynamic infrastructure, DynaWeb has a variety of channels to keep users updated. For example, a user can send a message to one of DynaWeb's instant messenger (IM) accounts, and will get an instant reply showing the newest addresses of DynaWeb portals. Similar things are being done with emails. By these many, dynamic channels, DynaWeb outsmarts any attempt to collect all DynaWeb addresses by the censors, because each user receives only a (different) subset of DynaWeb's addresses. Automatic blocking detection combined with quick reaction apparently frustrates the blocking efforts on the China side of the GFW.

DynaWeb also releases a tiny piece of software, FreeGate, which directly taps into DynaWeb's backbone and keeps a user connected to the dynamic channels automatically. There are indications that FreeGate has some capabilities built-in to exploit some zero-day vulnerabilities of the GFW.

In addition to its DynaWeb service, DIT has released numerous advisories and technical analyses of the evolving Internet censorship operations [http://www.dit-inc.us/press.php].

6.6 GPass and FirePhoenix

Recently two new kids have come to the block: GPass and FirePhoenix. Both were released in the summer of 2006 by World's Gate Inc. (WG). WG is an upcoming organization focusing on building an extensive and trustworthy Internet platform, Edoors (www.edoors.com), especially for users from repressive regimes. The objective is to freely and securely access and publish information, with support of the popular services such as emails, blogs, forums and social networks. As part of this offering, GPass and FirePhoenix (FP) are two anti-censorship systems that facilitate access to Edoors as well as other Internet services.

GPass and FirePhoenix set the trend of multi-protocol protection. Currently most anti-censorship tools only offer protection to web traffic, which means a user's privacy and safety are only protected when he/she visits those specific websites, but other applications with non-web protocols, such as emails, instant messaging, and audio/video streaming, are still subject to censorship.

GPass offers support of many application protocols, multimedia streaming (e.g., MMS protocol), file transfer (e.g., FTP), instant messengers, as well as web surfing (e.g., HTTP). GPass software provides users with an intuitive user interface for them to select which applications they want to be protected. GPass does the chores of finding and connecting servers, encrypting traffic and evading GFW without user intervention. It seems GPass has been built upon the experiences of Garden, UltraSurf and DynaWeb and did not have to reinvent many wheels.

FirePhoenix's way of censorship-busting is still more dramatically different from other existing tools. This is the first virtual private network (VPN) based anti-censorship tool. FirePhoenix is the most powerful protection offered so far to users working under censorship. After installation, the FirePhoenix software on a user's computer creates a virtual network card, and once FirePhoenix software connects to one of the numerous FirePhoenix servers on the other side of GFW, the virtual network card functions the same as a physical network card, but with the network cable plugged in the FirePhoenix server's local network. To a user, it is just as if his/her computers were directly connected to a wide open network overseas, and the GFW becomes nonexistent. The end result is that all of the user's Internet traffic is automatically protected, no matter if it is web surfing, chatting, instant messaging, audio/video streaming, interactive gaming, or any other traffic types or protocols. Even if some malicious reporting software is planted in a user's computer, FirePhoenix provides the most difficult environment for it to identify the host computer, as the report will appear to come from computers overseas.

Both GPass and FirePhoenix have proprietary technologies for server discovery. We have indications that these technologies effectively exploit undocumented weaknesses in GFW. Such exploits make the server discovery process simple and straightforward, avoiding many tricky issues other tools, such as Freenet, have to face.

Despite of their young age, GPass and FirePhoenix have quickly gained the trust of users and established a growing user base. Moreover, they joined the newly formed Global Internet Freedom Consortium (GIFC: http://www.internetfreedom.org), together with the top three anti-

censorship tools, Garden, UltraSurf and DynaWeb, to complement each other, to share technology, and to provide users with more reliable service.

6.7 Tor (The Onion Router)

Tor is also a relatively new addition to the anti-censorship arsenal. The project was originally supported by the US Naval Research Laboratory, and later inherited by Electronic Frontier Foundation (EFF) in 2004. The current development of Tor is largely community and volunteer-driven. The current stable release is 0.1.2.18.

Tor is a proxy chain. It counts on volunteers to run onion proxies (servers) on their computers. A Tor user installs the Tor client, which will route the user's traffic through an ad hoc cascade of Tor servers. The traffic between Tor servers is encrypted, so each server alone can not keep track of the end user. It supports TCP-based applications, but requires users to configure each application to use Tor's proxy service.

Since Tor is released as open source software, it has to face the dilemma of showing people how Tor works inside out while defying a censor's prying eyes. For example, Tor faces many challenges in enabling users to bootstrap in a heavily monitored environment[14]. As a matter of fact, Tor could be easily blocked by the Chinese GFW because the addresses of a few bootstrap Tor servers are explicitly hard-coded in the source code. In addition, it seems the developers are trying to reinvent wheels such as blocking detection, which has been a solved and in routine operation in many other services, such as UltraSurf and DynaWeb. Tor's multi-hop traffic pattern will also incur more latency than other single-hop proxy systems, but generally users in the censorship domains are more tolerant on this.

7 Operational Aspects

We emphasize here that technology alone is not enough to make a circumvention system successful. To turn such technology into valuable service, an anti-censorship system has to be run like a business operation. It is the operational quality and experience that eventually make a service stand out.

The daily operation of an anti-censorship system consists of the following aspects:

1. User support. Timely technical support for users is a must for a successful anti-censorship system. For example, five systems (Garden, UltraSurf, DynaWeb, GPass and FirePhoenix) are now sharing a unified technical support platform, www.qxbbs.org, which each system has its own user forum, where users can share their experiences and developers can provide technical support. For example, there are more than 20,000 posts on DynaWeb's support forum, with information ranging from technical tips, user

[14] Dingledine, R. and N. Mathewson: Design of a blocking-resistant anonymity system. http://tor.eff.org/svn/trunk/doc/design-paper/blocking.pdf

complements, and reports from China of new blocking test results. This operational area also includes internationalization, i.e., translation of user interface, documentation and instructions into users' native languages.

2. Marketing and promotion. Because anti-censorship software and its related information is naturally a target by censors, aggressive marketing and promotion are needed to get the word (and software) out via other channels so users can be informed and jump start. Successful conduits are emails, instant messaging, chat room and bulletin board posts. It is also highly effective when the anti-censorship systems can form an alliance and promote and protect each other, so a user can always have spare channels available to get new information or update their software when one particular system is blocked.

3. Monitoring and responses. The censors, especially the GFW operators, have been closely watching the leading ant-censorship systems, and responding with a dynamic blocking strategy in terms of its scope, scale and frequencies. Thus, it is critical to monitor the changing blocking situation and adjust the system at work accordingly.

4. Infrastructure support. When an anti-censorship system grows to a larger scale, the management of the whole computing infrastructure becomes a challenge. Without professional support to ensure stability, availability and scalability, it is impossible to support hundreds of thousands of users like Garden, UltraSurf and DynaWeb do today.

5. Content services. To better protect and serve users who have overcome the blocking and reached the other side of GFW, it is highly beneficial to provide them with an uncensored, trustworthy portal site in their own native languages, which provides services such as search engines, directories, bulletin boards, emails and chat rooms. These services are better protected when they are tightly integrated with the anti-censorship tools they use. More importantly, such a portal site can shield users from those overseas websites set up by the Chinese regime or communist regime-backed entities. Their websites serve as a trap to collect users' information as well as serve their exported propaganda machinery.

8 Impacts

These anti-censorship technologies and products have changed forever the Internet landscape in oppressive regimes. The social and political impacts they bring are hard to over-estimate. The increased failure rate of the Chinese regime's attempt to cover up critical issues is good evidence of our successes. Typical cases include the news reaching Chinese mainlanders of the SARS outbreaks in China, the arrests of dissidents, and the destruction of Christian churches. In addition, the inflow of uncensored information and perspectives from the free world challenge and often contradict the official propaganda, while stimulating independent and critical thinking.

Though the majority of these technologies and products are tuned for users in China, apparently the good news has traveled fast and far. Nowadays a significant number of Internet users from other censorship inclined countries, especially Iran and Burma, have discovered and adopted these products. For example, during the junta crackdown of the protests in Burma in September 2007, both UltraReach and DIT reported a surge of Internet traffic from Burmese IP addresses through their censorship-circumvention networks. The Burmese people were endeavoring to get the word out to the world when the junta jammed the Internet.

DIT also witnessed, through DIT's anti-censorship portal, Burmese posting on blogs the photos of protesters and the crackdown. If these anti-censorship tools are localized with native language support for the users in countries such as Iran and Burma, they will acquire much more popularity there.

9 Summary and Recommendations

Since the late 1990s a variety of technologies have been developed by grassroots organizations and volunteers, to challenge Internet censorship imposed by repressive regimes. In this article, we reviewed and evaluated the most influential anti-censorship systems, including the most operationally successful players (Garden, UltraSurf and DynaWeb), the promising newcomers (GPass, FirePhoenix and Tor), and the technologically innovative and influential ones (Triangle Boy and Freenet). Table 1 compares many aspects of these technologies.

Table 1. Comparison of Leading Anti-Censorship Technologies

	Start date	Current dev. status	Current est. user base	Ability to circumvent			Initial tunnel discovery	Speed	Access control	"Green" software	Chinese support
				IP blocking	DNS hijacking	TCP content filtering					
Freenet	1999	Active	~1000	Yes	N/A	Yes	Yes	Very slow	No	No	No
Triangel Boy	2000	Inactive	~0	Yes	No	No	No	N/A	No	No	No
Garden	2001	Active	~20,000	Yes	Yes	Yes	Yes	Fast	Yes	Yes	Yes
UltraSurf	2002	Active	~100,000	Yes	Yes	Yes	Yes	Fast	Yes	Yes	Yes
DynaWeb	2002	Active	~150,000	Yes	Yes	Yes	Yes	Fast	Yes	Yes	Yes
Gpass	2006	Active	~1000	Yes	Yes	Yes	Yes	Fast	Yes	Yes	Yes
FirePhoenix	2006	Active	~500	Yes	Yes	Yes	Yes	Fast	Yes	No	Yes
Tor	2004	Active	~10,000	Yes	No	Yes	No	Slow	No	No	No

The success of these technologies has proven that, despite their advanced technology deployment exemplified in the Great Firewall, Internet censorship systems can be circumvented and defeated. Nowadays, Internet users have available many alternative anti-censorship tools, and the censors have been kept too busy to track them all and develop countermeasures. Most

importantly, despite their close watch and intensive blocking, the censors have not been able to hinder the steady growth of technologies like Garden, UltraSurf and DynaWeb. In fact, the battle between these top tools and GFW has become well-known among Chinese users and their success stories have become effective advertisements for users.

By analyzing the achievement of the top systems, we conclude that the ingredients for anti-censorship success are new technologies and transparent operation. As this technology has become more mature and stable, we would argue that simple, practical operations are the key to success. In fact, the core technologies implemented in the most successful anti-censorship systems are not extraordinarily complicated. Actually, a too-sophisticated technology base may hinder a system's adoption by users, such as occurred with Freenet. It is a transparent operation that makes a tool stand out, and perhaps accounts for at least 70% of the success of an anti-censorship system.

We question the value of open source for developing anti-censorship technology in this particular field, because the business model here is not collaboration; it is competition and confrontation between censors and anti-censors. Keeping the adversaries in the dark can go a long way, as Garden, UltraSurf and DynaWeb have demonstrated. With no source code to study, the GFW operators have, apparently, not been able to figure out what tricks are up in the sleeves of these tools to penetrate their most reliable defenses.

As the anti-censorship technologies mature, the battle between censors and anti-censors is now ending up mostly as a resource battle. The leading anti-censorship system designs have the potential to support many more users than today. However, due to the limited human, computational and bandwidth resources available to the grassroots organizations and volunteers, the number of users they can support and the level of service are reaching a cap. Therefore, the anti-censorship community has been facing a Goliath of censorship with very limited resources at its disposal.

We urge government agencies, NGOs, and commercial companies to step in and back up these heroic efforts. Especially for democratic governments, many actions can be taken to bring the anti-censorship endeavor to a new level:

1. Provide resources to these efforts. This is the most effective support. Since anti-censorship technologies have matured and been field-tested, most of the resources would be devoted to the operation of these systems, instead of research and development. The impact of such support would be immediately visible.

2. Limit technology export to repressive regimes. Abundant evidence shows that the advanced Internet filtering technologies used in the Chinese GFW are provided by western companies[15]. Democratic nations should impose restrictions on such exports, which could be exploited for any future enhancements of GFW.

3. Eliminate the "trade deficit" of government propaganda. It is strange to see the government propaganda from China, direct or under various covers, enter freely into

[15] NTDTV, 2006: http://www.ntdtv.com/xtr/en/2006/11/23/a_47315.html

> democratic nations and spread misinformation, while the censors block information flow in the other direction, such as Voice of America (VOA)'s radio broadcasts and website. The infiltration of propaganda from the censors is harming the efforts of the anti-censorship community, as the users in repressive regimes see the disguised, misinformation on the other side of the GFW. Therefore, governments in free nations can pressure repressive regimes by imposing barriers to their propaganda exports unless the repressive regimes agree to stop blocking our information exports, like the VOA.

It is a challenging mission for grassroots organizations to bring freedom and privacy to Internet users in repressive regimes. We believe with support from government, NGOs and commercial entities, we will soon witness the fall of the Great Firewall, as we did the Berlin Wall.

Appendix. Common Concerns and Misconceptions

Due to the unique political, social, economical as well as technological environment in Net-policing countries, especially China, many people in the Western world have concerns and sometimes misconceptions regarding efforts to cripple the Great Firewall. Here we attempt to demystify some of them.

- *If the Chinese net police crank up their technology, they can totally block any censorship-circumvention traffic.*

Answer: They can block traffic with easy-to-identify patterns, but nowadays the GFW-penetrating traffic blends well with normal traffic. They can block traffic they have seen, but cannot block anything they have not seen. Based on our studies, many anti-blocking tools do not rely on single traffic flow. Some of them, for instance, FirePhoenix, has multiple, independent traffic streams, while others have backup channels which the net police have not seen yet. After all, it cost little to change a traffic pattern, but takes tremendous effort to analyze and implement blocking measures. This arms race favors the censorship busters.

More importantly, any technology is double edged. Whenever the censors scramble to deploy new counter-measures, they tend to inadvertently mess up other legitimate communications, such as the recent large-scale email service blackout in August 2007. Moreover, as the blocking technology is getting more sophisticated and sensitive, it is easy to trick it to misfire or trigger it to issue an unmanageable amount of false alarms.

We also want to point out that some people have tried to block some of these tools in a lab under isolated settings. No matter such an effort is successful or not, it does not imply these tools can be jammed in the wild. You can do anything you want to a lion in a cage, but you can not stop prides of lions running rampant all over African savannas.

- *What if the Chinese regime makes the anti-blocking software illegal and arrests everybody they find using the software?*

Short answer: Such a law would be the best advertisement for such software. Moreover, if their laws have not stamped out software piracy, no laws will be effective enough to stop the use of free, anti-blocking software.

Long answer: Wary of international exposure, the Chinese net police have largely carried out the censoring operation underground, and have not officially admitted the censorship of free speech of the Internet. A law to make anti-censorship software illegal would uncover the business they have claimed not to be doing. In addition, such a law could greatly arouse the curiosity of the Chinese users and lead to an avalanche of new users trying it out.

A book entitled, “Nine Commentaries on the Communist Party” illustrates this unique social phenomenon in China. This book reveals the corrupt, violent, and deceitful nature of the Chinese Communist Party (CCP), a collection of historical facts and accounting of its crimes during the past half century which the CCP has tried hard to cover up. This book has been

circulating underground in China since 2005, and the CCP is fully aware of the threat, and has been scrambling to launch a low-profile crackdown of the circulation. However, the CCP never tries to publicly condemn or make the book illegal, fully knowing that such actions would greatly speed up interest and circulation.

- *If their computer experts study it hard, they will eventually be able to throw a monkey wrench into your software and stop its spreading.*

Answer: If so far the whole computer industry has not been able to wipe out computer viruses, it is virtually impossible to stop a piece of software which users willingly pass along to each other.

- *How do you get your software into users' hands in the first place?*

Answer: Various anti-censorship groups can cooperate and complement each other. In fact, Garden, UltraSurf, DynaWeb, GPass and FirePhoenix are forming a consortium to join forces. Users can use one tool to get another, and the user base for these five tools has already reached the critical mass. Therefore, bootstrap is not an issue.

In addition, the anti-censorship groups have been proactively promoting their software via other channels, including snail mailing of CDROMS, emails, downloads via instant messages, etc. In fact, the demand for such software has prompted selling of CDROMs containing such software packages on the streets in China, right next to pirated DVDs.

- *What if the anti-blocking software is used by terrorists?*

Answer: Anti-blocking software is not an end-to-end encrypted communication system. It is a half-open tunnel. Once a user's traffic evades the GFW and reaches the open Internet, it is in clear text. In addition, user activities can be monitored on the servers if needed. Therefore, it would be the last choice for illicit applications.

About The Global Internet Freedom Consortium

Formed in 2006, the Consortium is an alliance of organizations that develop and deploy anti-censorship technologies for Internet users residing in oppressive regimes. The Consortium partners have contributed significantly to the advancement of information freedom in China. The anti-censorship technologies which the Consortium members developed have enabled Internet users in China to securely visit websites blocked by the Chinese regime, such as those of Voice of America and Radio Free Asia. For more information, visit http://www.internetfreedom.org .

NOTE:

This white paper is also available online at the following URL.
http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf