Formed in 2006, the Global Internet Freedom Consortium (GIF) is an alliance of several leading organizations that are developing and deploying anti-censorship technologies for Internet users living under oppressive regimes. The Consortium partners have contributed significantly to the advancement of information freedom in China, Iran and other “censorship” countries.

Two of GIF’s most popular anti-censorship software tools, *FreeGate* and *UltraSurf*, have played a critical role in enabling Iranians in the recent election aftermath to connect and communicate over the Internet when their government blocked most overseas news and social networking websites overseas. It is estimated that, on June 20, 2009, alone, over 1 million Iranians used GIF to visit previously censored websites.

In addition, GIF itself has constantly been fending off cyber attacks launched against it. 

UltraSurf is a flagship anti-censorship product by UltraReach Internet Corp. (www.ultrareach.com).

On October 22, 2009, the U.S. Congressional Commission on Security and Cooperation in Eurpoe, also known as the U.S. Helsinki Commission, held a hearing on the ways in which new media and Internet communication technologies affect the balance of power between human rights activists and authoritarian governments. Zhou Shiyu, Deputy Director of GIF provided testimony at the hearing. Zhou estimated that over 90% if anti-censorship traffic comes through GIF servers. GIF has the current capacity to support 1.5 million people per day. It is working on expanding its capacity to meet the rapidly growing demand.

Chinascope recently interviewed Dr. Peter Li, GIF's Chief Technology Officer:

Chinascope: Recently President Obama launched the cyber security plan. Are cyber attacks a real threat to U.S. national security?

Dr. Li: Definitely, especially the cyber attacks from foreign governments.

Chinascope: What are the current characteristics of cyber attacks?

Dr. Li: There has been a strategic shift since four or five years ago. Nowadays the attackers do not pursue instant gratification, such as defacing a government website. Instead, their strategy is more systematic and well-planned.

For example, when they hack into a website, they do not deface it. Instead they insert a couple of lines of malicious code into every page. When you visit this website, the malicious code will exploit the vulnerabilities in your browser and install spyware, which can log your key strokes to harvest passwords to your email accounts. Then the attackers hack into your email accounts with the stolen password, and study the communications between you and your contacts. Armed with such information, the attackers then impersonate you and send emails to your contacts with the correct context, but with malicious attachments. Your contacts are then tricked into opening the attachments, and their computers are planted with spyware too. So goes the cycle.

Chinascope: How to defend?

Dr. Li: Such attacks are really hard to defend. Especially when you have tens of millions of computer users, it is always easy to find a few weak links among them. Nowadays, everyone on the Internet is so highly connected, probably with much fewer than six degrees of separation. The attackers can almost be guaranteed to find a link to be able to invade, whether it is a plumber’s computer or a missile designer’s.

It is also hard to launch pre-emptive attacks. Besides messy legal and political hurdles, it is technically nearly impossible to identify an adversary's presence in cyberspace. If a computer's cable is uplugged, it is simply not visible on the Internet. Once plugged in, however, it can wreak havoc from thousands of miles away. You are fighting against ghosts.

Chinese communist regime is 'biggest player'

Chinascope: Who is behind the cyber attacks against GIF?

Dr. Li: There are good reasons to believe the Chinese Communist regime is the biggest player behind the curtain. We have experienced their attacks against the information systems of GIF, Falun Gong and Initiatives for China firsthand. The recent discovery of GhostNet sheds additional light on it. Who else is so interested in attacking GIF, Falun Gong, the Dalai Lama, Initiatives for China and other Chinese dissident groups?

However, we also believe that GIF, Falun Gong, and the dissident groups are only their practice targets. The Chinese Communist regime has already deployed and attacked extensively in cyberspace. We all have seen reports of defense contractors' computers having been compromised. The attack tactics were exactly the same as those they used to attack us. Their goal is global information superiority: they want to know your every plan and every move way ahead of time.

Chinascope: Will President Obama’s cybersecurity initiative be effective?

Dr. Li: It is a good start, but as far as defending the U.S. from the Chinese Communist regime's strategic attacks, it is missing a critical dimension. The critical dimension is to overcome the Great Chinese Firewall and open up the Internet to all of China's people, thus making cyberspace more transparent.

Chinascope: How does this help?

Dr. Li: A key element the Chinese Communist regime relies on to maintain its power is propaganda. It is apprehensive about information freedom, and the Internet is now the best media for this. That is why it has built the world's most powerful firewall, not to defend itself from outside attacks, but to confine the Chinese people inside and to hamstring their ability to obtain information.

We who were brought up in China all know what it was like; how the Communist education system cripples people's ability for independent and critical thinking; how it cultivates hatred toward Western civilization and makes people believe democracy is not good for China; and how we are brainwashed with a "purified version" of Chinese history so that college students have no knowledge of what happened 20 years ago at Tiananmen Square. For example, nowadays many college kids in China are led to believe that the United States is the biggest impediment to China's "Peaceful Rising."

Under this climate, it is easy to breed, recruit and use the young, rich in technical skills but poor in independent thinking capability.

The ultimate purpose of blocking information flow, or attacking/spying in cyberspace, is the same – maintaining the Communists' hold on power.

But we have seen the changes that the Internet has brought in the past ten years, especially with the anti-censorship services GIF has developed and which are now widely enjoyed by millions of users in China, to penetrate the Great Firewall and enable the outside world to be seen. As a result, we have started to see, even within the tight Chinese web sphere, how official voices are questioned or even ridiculed, authorities are challenged, and history is being rediscovered. If the fall of the Berlin Wall predates the collapse of the Soviet Union, then we believe the fall of the Chinese Great Firewall will dissolve the Communist regime and its cyber aggressiveness.

This tiny GIF has done so much. Imagine if this endeavor were amplified one hundred or one thousand times. The impact would be huge. This is the best pre-emptive attack – no legal or political hassles, no secrecy, just open promotion of Internet freedom for the Chinese people, who have been so passionate about our services. Ghosts cannot live in sunlight. Such an initiative needn't even be portrayed as an attack against China, but can be portrayed, accurately, as a positive U.S. commitment to provide information freedom for the residents of all of the world's closed societies. The accuracy of such a need can be seen from the fact that GIF systems are being used by residents of Iran, Burma, Syria, Laos, Vietnam, Cuba and by the residents of all societies where the government monitors and censors the Internet.

Having said this, however, the point is still clear that when the Chinese Communist system disappears from the physical world, we will see a much more peaceful cyberspace.

Chinascope: Can GIF directly fight back cyber attacks by hacking the ghosts?

Dr. Li: No, that is not what GIF is for. We do not hack into people's computers, in China or anywhere else. We just provide tools for users to securely obtain censored information. We think empowering end-users with information freedom is more productive.

Chinascope: On the other hand, can terrorists exploit GIF to attack the U.S.?

Dr. Li: No. To the best of our knowledge, GIF's anti-censorship system is the only one with the capability to block terrorist or other illegal activities. In contrast, nowadays it seems there are a few social-network-based anonymity systems out there, which route Internet traffic through many end-user computers in the U.S. or other censorship-free counties. Such a system design does not have effective mechanisms to prevent abuses. The end users who help to route traffic will soon be plagued by claims that illegal online activities such as identity theft, credit card fraud and child pornography are originating from their computers. We have seen this result from GIF's own experiments. So our operational system does not suffer from such vulnerabilities. GIF's services will be the last choice of terrorists or other cyber criminals.

Chinascope: What do you recommend the Obama administration do specifically?

Dr. Li: This administration should invest substantial effort in opening up the Internet to people living in censorship countries, and in doing so, make cyberspace more transparent. The Internet should, as it was originally designed, enable better connections and communication among people regardless of physical distance or national borders. It should not be used by repressive regimes to manipulate information flow and cultivate hatred against the Western world. Strategically, it is critical to cyber security and to U.S. national interests.

Download the latest software from Global Internet Freedom Consortium website