

**Statement of Paul Baranowski**  
**China's Cyber-Wall: Can technology break through?**  
**November 4, 2002**

I am the project leader of Peekabooby, a piece of software that is designed to get around state-sponsored Internet censorship at the national level. Peekabooby accomplishes this using peer-to-peer technology. Peer-to-peer (P2P) basically means that there is no central authority governing some part of a networked system. The idea is that anyone that uses a P2P system also helps out others. Napster, Gnutella, Morpheus, and Kazaa are all examples of peer-to-peer networks. Peekabooby uses other nodes in the network to relay data around the firewall, kind of like a distributed proxy service.

China has been working on its firewall since before 1997, and we have seen its power growing over the years. Just about every other month now we see another story of a new technology being implemented in order to more effectively filter information.

The Chinese authorities started by blocking web pages based on their Internet Protocol (IP) address. Citizens of China initially worked around this by using "open proxies" - that is, other computers on the Internet that indirectly fetch web pages for the user. In early 2001, the Chinese Communist Party countered the use of open proxies by scanning the Internet for them, and adding the proxies to their banned list. Web sites have also responded by changing their IP addresses. However, they can only change their IP addresses every few days and this costs money, so this is fairly ineffective.

SafeWeb and Voice of America (VOA) set up a system that would send the IP addresses of available proxies to whoever requested them. However, it wasn't long until the Computer Monitoring and Supervision Bureau of the Ministry of Public Security started requesting the proxy addresses and simply banned any IP addresses it received.

There are two strategies that have not been effectively countered yet: bulk email lists (where email is sent out to an enormous number of people) and Freenet. Bulk email still works because the origination of the email is different every time. However, email has the drawback of being one-way communication. Freenet is a peer-to-peer system that allows two-way communication, and it still works because the only way to find another Freenet node is through "out-of-band" means. This means there is no automatic way to discover all the nodes in the network. The only way to find another node is, for example, by calling up a friend of yours that is running Freenet and getting his IP address or having an IP address personally sent to you in an email.

One of the main goals of Peekabooby is to overcome this limitation: to create a method of discovery that is automatic yet never allows anyone to discover all the nodes in the network. I am currently developing a simulation of a system that shows great promise in this regard.

More recent developments of the Chinese firewall include:

- Selectively blocking out content within a web site instead of blocking the entire site
- Denying internet access for a certain amount of time to anyone searching for a banned keyword
- Suppressing dissident comments in chat rooms, followed by a warning email to the user who made the comments
- Logging Google keyword searches

We can do something about this if we act now. The Chinese government is already on its third generation of firewall technology, and we haven't even started version one of our counter-strategy yet. If we do not do something soon, they may be able to close off the country completely and obtain absolute monitoring and

control of their net before we can do anything about it. A fair guess is that by 2008, when the Olympics go to Beijing, it will be much too late to act. Our window of opportunity is now, at this moment.

The US government is the only organization that has the power to mount an effective counter against this type of censorship. Independent efforts by volunteer groups will be ad-hoc, and there will be no coordination between the releases of the various projects. A well-funded, centralized program could plan application releases so that they occur at regular intervals in order to keep the Chinese authorities constantly scrambling to keep up. In other words, the U.S. agency in charge could coordinate and plan a global strategy that would be much more effective than the current ad-hoc state of affairs. Centralizing this type of activity also allows for the possibility of interoperation between the projects, allowing more advanced features in each product and eliminating redundancy.

There are few, if any, commercial possibilities for this type of software, which is why the government is the only organization with the power to fund this kind of activity on the scale that is required. The amount of money proposed in the Global Internet Freedom Act has the possibility to fund dozens of projects. There are so many aspects to this problem and so many ways to solve it that this is the kind of depth we need. Research is just beginning on this subject and we have a long way to go. This panel represents a sample of what is out there - there are, perhaps, on the high end, a dozen grass-roots efforts attempting to do something about this on a shoestring budget. However, this is not as many as we need. Right now development on all of them is extremely slow due to the fact that they all rely on volunteers, usually only one or two per project. The first thing that is gained with funding is development speed. With a full-time staff working on each project we would see rapid improvements in the technology. The second thing that we gain is usability. For your average consumer, the user interface is everything. For developers, this usually comes last. With appropriate funding, experts can be hired to solve the usability problem. Third, the interface for each program must be translated into various languages, most importantly Chinese. With funding this becomes possible. Finally, marketing the applications to their intended audience is critical. Some part of the funding for each project should be spent on promotion.

If the US government does fund projects such as these, it should be done through credible organizations that are committed to developing open-source solutions. Open-source software is crucial, due to fear of software backdoors that would allow remote monitoring or tampering of a user's computer. Open-source software relieves these fears because the code can be vetted by outside experts.

One of the important things about many of the current projects is that they use peer-to-peer technology. In terms of cost, this means that they do not need large amounts of cash to keep them running. Funds are mainly needed for maintenance of the code and the addition of features. Each project could be initially funded by only a few hundred thousand dollars a year, and even less for maintenance once they have been deployed.

The current crop of anti-censorship projects that show promise and should be considered for funding include the following: Peekabooby, Freenet/Freenet-China; the Invisible IRC project (IIRC) which allows anonymous chat; CryptoMail, a web-based email system like Yahoo that provides automatic encryption of email; and Pretty Good Privacy(PGP) and Gnu Privacy Guard(GPG) plug-ins to email clients (examples of such plug-ins are enigmail and Kmail).

It should be noted that the National Science Foundation (NSF) has started funding anti-censorship research at the academic level. What we need is a system to transfer the research into real world applications. One of the areas of research that has not yet been exploited is in the field of wireless networking. This technology would allow wireless devices to route information on their own. If there was an application that did this, and enough wireless devices, it would create a new Internet infrastructure which could not be filtered. I also think there should be work done to make email encryption easier to use and more transparent.

China's censorship technology is becoming more advanced every day. We can do something about it, but we must act now. The government should fund credible third-party organizations to develop open-source anti-censorship technology. Multiple strategies should be developed and their release should be coordinated according to a centralized high-level strategy. If we do not act, there is no doubt the Chinese Communist Party will have more power over its populace than ever before in history.