CHINA'S CYBER-WALL: CAN TECHNOLOGY BREAK THROUGH?

ROUNDTABLE

BEFORE THE

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

NOVEMBER 4, 2002

Printed for the use of the Congressional-Executive Commission on China

Available via the World Wide Web: http://www.cecc.gov

U.S. GOVERNMENT PRINTING OFFICE

83–512 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

LEGISLATIVE BRANCH COMMISSIONERS

Senate	*House*
MAX BAUCUS, Montana, *Chairman*	DOUG BEREUTER, Nebraska, *Co-Chairman*
CARL LEVIN, Michigan	JIM LEACH, Iowa
DIANNE FEINSTEIN, California	DAVID DREIER, California
BYRON DORGAN, North Dakota	FRANK WOLF, Virginia
EVAN BAYH, Indiana	JOE PITTS, Pennsylvania
CHUCK HAGEL, Nebraska	SANDER LEVIN, Michigan
BOB SMITH, New Hampshire	MARCY KAPTUR, Ohio
SAM BROWNBACK, Kansas	SHERROD BROWN, Ohio
TIM HUTCHINSON, Arkansas	JIM DAVIS, Florida

EXECUTIVE BRANCH COMMISSIONERS

PAULA DOBRIANSKY, Department of State
GRANT ALDONAS, Department of Commerce
D. CAMERON FINDLAY, Department of Labor
LORNE CRANER, Department of State
JAMES KELLY, Department of State

IRA WOLF, *Staff Director*
JOHN FOARDE, *Deputy Staff Director*

CONTENTS

CHINA'S CYBER-WALL: CAN TECHNOLOGY BREAK THROUGH?

MONDAY, NOVEMBER 4, 2002

CONGRESSIONAL-EXECUTIVE
COMMISSION ON CHINA,
Washington, DC.

The roundtable was convened, pursuant to notice, at 2:30 p.m. in room SD–215, Dirksen Senate Office Building, Ira Wolf (staff director) presiding.

Also present: William Farris, senior specialist on Internet issues and commercial rule of law; Keith Hand, senior counsel; Holly Vineyard, U.S. Department of Commerce; and Dr. Jay Sailey, interpreter, Silver Spring, MD.

Mr. WOLF. I would like to welcome everyone here to today's roundtable on China's Cyber-Wall: Can Technology Break Through?

This is actually our second roundtable this year dealing with Internet issues in China. The first dealt more with policy issues, and today we are going to get more into the technology side.

Next to me is William Farris, who is on the Commission staff and is in charge of Internet issues. Holly Vineyard works at the U.S. Department of Commerce for our Commissioner, Under Secretary of Commerce Grant Aldonas, and Keith Hand is one of our senior legal counsels on the Commission staff.

I am Ira Wolf, staff director of the Commission. John Foarde, who is the deputy staff director and normally would be here, is in China.

We have four panelists. Avi Rubin is co-founder of Publius; Bill Xia, president of Dynamic Internet Technology; Lin Hai, a computer scientist from Shanghai; and Paul Baranowski, chief architect for the Peekabooty project.

We also have Jay Sailey, who will be helping with interpretation. Jay, it is good to always have you back again. Thanks.

Avi, why do we not start with you?

STATEMENT OF AVIEL RUBIN, CO-FOUNDER, PUBLIUS WEB PUBLISHING SYSTEM, WEST CALDWELL, NJ

Mr. RUBIN. Let me give a little more of an introduction of myself. I want to give you an idea of the kinds of questions I am hoping to get and the kinds that I will defer to my other panelists.

I am a researcher at AT&T Labs, a computer science background. I am here explicitly not as a representative of AT&T, but as a computer scientist.

In January, I will be starting to work in a faculty position as an associate professor at Johns Hopkins, and the technical director of their Information Security Institute.

The reason that I am here is that some of my research in the past that focuses on computer security and networking has been on systems that resist censorship. One of them called "Crowds" was designed for browsing the Web anonymously so that end users and other users of the system cannot tell who is accessing what.

The other system, called "Publius," which has won a censorship resistance award and is a little better known, was designed to publish information on a large network like the Internet in such a way that it is very difficult for anyone to forcibly remove the content.

I am not an expert on China and I would rather answer general questions, such as, "Is this possible? Is that possible? Why or why not?"

So let me talk a little bit about censorship. I think it is important to make a distinction between censorship within a network or within an organization or a country and censorship between users who are on the inside trying to access something that is on the outside where an adversary controls the interface between the inside and the outside, which is the kind of model that we are looking at here.

The censor can prevent access to content on the outside through several means. One of them is simply by routing, looking at the Internet Protocol [IP] addresses of the destination of a request, and if it is on the outside, perhaps blocking that or filtering it some other way, or making a decision about how to treat that traffic differently.

Another way would be through use of the domain name system. For those of you that do not know, the domain name system is the service that translates names like www.google.com into an IP address that networks need in order to get the packets where they need to go.

So one thing that a censor could do, and I believe in a lot of cases this happens not only for censorship but for other purposes, is if the organization controls the domain name service [DNS]—and a powerful government can control the domain name service, or at least control those that control it—you can return false information, so when someone asks for google.com you can return an IP address. This will all be transparent to the users.

That is an IP address to a computer under your own control, which could then simulate Google, giving the user the experience that they think they are at Google, but they are actually at some other, mirroring network. This would be a censorship technique that could be employed, or could simply drop the traffic or do whatever they want with it.

Finally, you could do something called application level filtering. Instead of doing the censorship at the routing level or the domain name service level, what you could do is allow all traffic through. But, if it is destined for port 80, which is the World Wide Web port, then you could treat it differently.

You could make filtering decisions and you could run it through software that looks for particular destinations, compare it to a blacklist and say, well, we are not going to allow that, or worse,

we are going to substitute something for that in the reply, spoofing the reply.

So, this has had to do with blocking the access of an individual within an organization to sites that are outside the organization.

Another type of censorship is prohibiting the posting of content. I am an individual and I have something that I wish to have people access. Maybe I have some agenda that I want to publicize, or I want to be critical of the government, or whatever. A censor may wish to block the ability of somebody to post the content.

One way to do that would be to monitor sites carefully using search engines or hot lists, and see if content that is objectionable is there, and then to go make the people remove it if the content is on the inside.

Another, is through informants or spies who could infiltrate organizations that may wish to publish something that they would find offensive, and then finding out that it is there and doing the same thing.

Again, if you control the connectivity, you can prevent someone inside your organization, your country, or China from being able to publish something that is in a site that is outside by simply blocking the connectivity or making the decision not to allow that.

So what I have discussed up to this point is a one-to-many censorship. Somebody publishes something on the Web, say, and you either block their ability to publish that or you block people's ability to retrieve that information.

Another type of censorship would be one-to-one communication. Someone may want to monitor e-mail messages that are going from one individual to another, and there are various ways of doing that.

The FBI has a system called "Carnivore" that can be deployed at an Internet service provider [ISP]. What it does is it searches e-mails coming in and out for certain key words, looking perhaps for terrorist activity.

The Chinese Government could deploy similar things at ISPs. In fact, they probably have more control over what the ISPs are doing, and look for whatever it is that they are interested in blocking. Then they can take whatever actions they want. They could block those e-mail messages. They could try to trace the owners of the accounts who sent or received those.

Another thing that could happen to e-mail is, again, an application-level way of censoring. At the network level, what we call the IP layer, you could sniff. Network sniffers are programs that will look at packets coming in and out and make the same kind of decisions that were made at the application level about the e-mail by just looking at raw IP packets.

It is a bit harder to do, but there are tools out there to do it. You take a bit of a performance hit when you do it that way, but the advantage for the censoring party in doing it that way is that it is completely passive. The ISP does not need to know that this kind of sniffing is taking place. Nobody can detect that it is happening.

Another way to censor the one-to-one communication is to forbid encryption. If encryption is not allowed, then something like Carnivore or network sniffing is very effective.

What sort of enforcement could take place if censorship were to detect that somebody had offensive content posted somewhere?

When something is published, it resides in a physical place. It is on a computer. If that computer is under the domain of the censor, the censor can apply pressure to the administrator, or sanctions to the administrator of that computer and say, "take that content down."

Finally, a way of censoring content might be to mandate a custom client. Instead of a Netscape or Internet Explorer browser, a government could say, "We require you to use this program to browse the net," and that program could be some sort of scaled-down version that can only access certain approved sites.

So up until now I have talked to you about ways of censoring. Let me speak, for my remaining time, about types of circumvention that you might have.

One, is called steganography. The idea behind steganography is to hide content in other content. Briefly, imagine a photograph of your cat encoded as a JPEG image on a computer.

There are tools out there for you to take a letter, an ASCII text letter, and encode the content of that letter in the picture of the cat, which still will look like a cat. And the only people that could extract that information, the letter from this picture, would be someone who knew the key, say, that you had shared with them.

In fact, there are techniques where two photographs are indistinguishable relative to whether or not they contain content to anyone except the holder of the key. So, this might be a valuable technique to use if encryption is outlawed and you are worried about sanctions.

On the other hand, if someone does discover the key through force or through some other means, then you could be in a lot of trouble, because once they extract the letter that could not have been coincidental.

Another way is to disperse content widely. If you want to publish something and you have an automated way of publishing it in a thousand places, it becomes a lot harder for a censor to remove it, especially if these are under different administrative domains and countries.

The Publius system that I designed and built uses the last two techniques in tandem, along with several others. I am happy to cover it more during questions and answers.

Two other mechanisms for circumventing the censorship to post something are covert channels. A quick example of a covert channel might be, let us say that I was to communicate a message to you. So what I do is send you an e-mail message every second, or I do not send you an e-mail message every second, and whether or not I send you a message encodes a zero or a one.

That is just a very lightweight example of how I could communicate information to you where I am actually using a covert channel. The fact that I sent something or did not send it is the information, and whatever it is that I sent could be just innocuous.

Finally, there is a technique called a homomorphic encryption. That is a mechanism whereby you can encrypt something so that it can be decrypted two different ways. So I send you an encrypted document.

Of course, only a regime that allows encryption would support something like this. You can decrypt it and it is a picture of your

cat, and you can decrypt it and it is a call to arms. It depends on how you decrypt. So, that might be useful.

For retrieval. I am running out of time, so I will just enumerate the things you could use. Special proxies, the Crowd system, which I can talk more about in the questions and answers, or an anonymous location, a library, a cafe, something like that if the country supports these kinds of things.

Finally, let me just say that I believe there is an arms race between censorship and censorship circumvention, because if you tell me what you are using to censor I can tell you what to do to get around it. But, once I do that, then I could come back and tell you what you could do to get around that. I think we are in the midst of this arms race.

I believe that any technology to circumvent censorship, having had the experience of developing such a thing, is going to lead to a double-edged sword where you could be accused of providing mechanisms whereby bad people can also do things.

[The prepared statement of Mr. Rubin appears in the appendix.]

Mr. WOLF. Thank you very much.

Bill Xia.

STATEMENT OF BILL XIA, PRESIDENT, DYNAMIC INTERNET TECHNOLOGY, INC., CARY, NC

Mr. XIA. Good afternoon, ladies and gentlemen. I would like to thank William Farris for inviting me to come here today.

My name is Bill Xia. I am the president of Dynamic Internet Technology [DIT]. DIT conducts research regarding Internet censorship and provides service for anti-censorship technologies.

Today I would like to share with you the experience of DynaWeb and ponder upon the role of technology in breaking through China's cyber-wall.

DynaWeb was launched on March 12, 2002 as a proxy network that allows users to circumvent Internet censorship in China and to have secure and full access to the Internet.

Users can use DynaWeb as an information Web or to go to other Web sites. Since the inception of DynaWeb, we have managed to stay ahead of the censorship by China most of the time. About 20,000 unique users gain regular, unblocked access to the Internet through us.

DynaWeb has already played several rounds of the censorship and anti-censorship game in the past 8 months. Before I start, I would like to explain a few critical technical terms for understanding the DynaWeb experience.

There are two ways to access a Web site through an Internet browser. One, is through typing the domain name, for example, google.com. The other way is through typing the IP address of the domain name. The IP address is the essential element from which the browser can fetch the Web site information for the user.

However, a domain name is more user friendly. After a user types in a domain name, the Web browser will browse domain names to IP addresses and fetch the right information for the user. So this is essentially what Mr. Rubin explained about the DN system.

The game started with an e-mail subscription service. At the beginning, DynaWeb e-mailed unblocked IP address updates to subscribers. After 2 weeks, the censor probably subscribed to our e-mail service as well because the very time window of DynaWeb IP addresses was reduced a range of a couple hours to a few days after release.

Then our services expanded to the domain name with Dynamic IP addresses. However, censors started chasing the DynaWeb domain by automatically detecting the IP addresses that pointed to the domain name. This dramatically increased the need for back-up IP addresses, hence, increased costs of DynaWeb maintenance.

Then DynaWeb adopted a new strategy so that censors had to manually verify the IP address before blocking it. Then automatic IP blockage stopped.

Soon, in August, users started to have difficulty in accessing DynaWeb through https, even though the IP was not blocked. It was found out later on that the certificate DynaWeb used for secured access from the Internet browser was filtered. This can be achieved by package-level analysis of Internet traffic to find out the signature related to the certificate DynaWeb used.

In response to this, DynaWeb started to change its certificates daily. No reports of certificate blocking have been found since then. Again, censors were frustrated with the resources required for daily updates of all related content filtering engines, and quit.

At the end of September, DynaWeb domain names were hijacked to a fixed IP 64.33.88.161 in China, along with many other Web sites like www.voa.gov. DIT has published a detailed report about this hijacking and it can be independently verified from the United States. More study about this hijacking is still ongoing and will be released after we pass this stage.

So what is next with the cyber-wall? As a first look, it is a technical question. If technology can break through China's cyber-wall, in fact, the process is a race of technology and time. As DynaWeb's experience has demonstrated, both parties can always implement new technologies to stay ahead and sustain the advantage.

If the Internet breakthrough is defined as a pure technical issue, the future is brighter for censors because China purchases the most advanced censorship technologies from Western companies.

China is also developing the "Golden Shield" project, a "database-driven remote surveillance system." When the whole Beijing city is wired with a biometric sensor and camera network, no Internet-based anti-censorship can get around the surveillance system.

Even now, during the 8 months of the technical race with DynaWeb, China has developed the largest and most sophisticated IP blocking and content filtering system in the world.

The more anti-censorship techniques are developed, the more comprehensive censorship technology has become. This leaves less and less technical room for anti-censorship. So, it is critical to take full use of technologies to benefit as many people as possible before the door is closed.

Second, it is a matter of available resources. China has 30,000 Internet police that specialize in Internet censorship, and ISPs are forced to perform self-censorship. The self-censorship is even adopted by foreign ISPs such as Yahoo.

China has purchased top technology from Western companies. These technologies have been modified for China's particular censorship needs. Nortel, Sun Microsystems, Cisco, and many smaller companies contributed to building China's cyber-wall.

Compared to China's investment in censorship and the cyber-wall, investment in breaking through this cyber-wall is next to nothing. There are very few groups developing technologies suitable for this wall. With more resources, DynaWeb can provide services to more people, develop better client software, and have closer monitoring of censors' new technologies, and respond faster.

Third, people develop technology and technology serves people. The people factor is the most important factor, eventually. Recent increase of public awareness about China's Internet censorship both inside and outside of China is a great sign. We hope that this will help improve the current situation soon.

Currently, companies contributing to China's cyber-wall bear little public pressure, not to mention any legislative limitation.

Inside China, more and more harassment and arrests of dissidents and journalists are related to the Internet. Last year, there were more than 10 arrests in China for distributing forbidden information. This will create fear among the public. For the general public in China, they are now gradually realizing the existence of censorship consciously.

More importantly, the government has adopted subtle mind control and propaganda to decrease the Chinese's interest in uncensored information. All major events outside of China are reported, with seemingly a variety of views, although all the different views are in fact the government's view. There is a fully developed online community inside China serviced by self-censoring ISPs. This strategy is an extension of China's cyber-wall, a wall in people's minds.

The Internet, combined with TV, newspapers, and other information channels, now offer the Chinese people different types of information and different views on certain issues. It looks like full freedom of speech has been achieved.

However, the government produces all the different views and types of information. The censors tried to use these to reduce people's interest in uncensored information.

In summary, technology alone will not decide the future of China's cyber-wall, but people do. If all Chinese people would like to obtain uncensored information, the cyber-wall will be broken from the inside.

Thank you.

[The prepared statement of Mr. Xia appears in the appendix.]

Mr. WOLF. Thank you very much.

Lin Hai.

STATEMENT OF LIN HAI, COMPUTER SCIENTIST, SHANGHAI, CHINA

Mr. LIN. Ladies and gentlemen, good afternoon. My name is Lin Hai. I was born in Shanghai, China and graduated from Beijing's University of Aeronautics. I majored in computer science.

After graduation, I worked as a software engineer, as well as sales marketing in some technology companies in Beijing for more than 5 years.

At the end of 1995, I went back to my home town, Shanghai, and created a small Internet company with my partners. Our major business was to help other people to set up Web sites. Our major clients are joint ventures and foreign companies who are in business in Shanghai.

As one of the first Internet users in China at that time, I was involved with the Internet Society, as well as technology because I, myself, was an Internet engineer.

As was my interest, I did some technology research. For example, at that time I collected a lot of information on Chinese Internet users to see who was using the Internet, just for my own interest.

Also, I was very excited about this new technology and expected some possible changes to the society by the new technology.

I received a letter from a U.S.-based student's organization. The organization publishes newsletters that promote democracy, freedom of information, and independent opinions, as well as news into Mainland China. I was so excited because it was the first time that people could have a media that is not censored by the central government.

So, I did something to help the organization, especially to help them in collecting information on Chinese Internet users so they could promote their newsletters to more receivers.

For that activity, I was arrested by the Chinese Government. The date was March 25, 1998. As reported, I was the first victim of China's censorship of the Internet. So, I thank this Commission for letting me have a chance to speak here to all of you nice people.

After I was arrested, my case was reported online. Finally, the government closed the trial and sentenced me to 2 years for some political crime. Thanks to the media reporters and many other supporters from outside organizations, especially human rights organizations, the Government of China released me early, with only 6 months to go. So, actually, I stayed in jail for a total of 18 months.

After I was released, I stayed at home and tried to find some chance to re-start my business or career. I failed to do that because China is still a Communist country.

So, for reasons you can probably understand, I found that I had to leave the country to seek my opportunities. So, I came to the United States. Right now, I am working in a small Internet company in New York City doing similar jobs as I did before as an Internet engineer. That is all of my story.

Right now, we are doing a project named "Secure Email Proxy," an Internet proxy project. The background is that people in China try to get free information. The Web sites on democracy are all blocked by the Chinese Government.

E-mail seems to be an option for receiving information. E-mail is a traditional application on the Internet, and they are still using it daily. It is proven to be easy to use and cost effective.

People in China can receive information from those independent sources by subscribing to e-mail newsletters and some other organizations who send e-mails.

It has worked in the past few years. Some months ago, something happened. As before, the Chinese Government has filters at almost all major IPs in China. Those filters check every e-mail that comes in to China, to check if there are any key words encoded in

the e-mail. If they find more than, for example, 10 key words in an e-mail, they will block this e-mail and the people will not receive it. Furthermore, it may be dangerous to the receivers.

So, clever Chinese people found that they can use free e-mail boxes such as Hotmail and Yahoo Mail, which are based in the United States. It is out of the control of the Chinese Government. They can subscribe to those sources with their free e-mail account.

It worked for years. But several months ago, the Chinese Government developed new technology that not only filtered the e-mails themselves, but also filtered the normal Web pages. If people in China accessed an e-mail box, say, Hotmail, it really works like a normal Web page on the Hotmail Web server.

The Chinese filters—they installed filters on the gateway, I think—if people access a Web page that contains key words, the whole Web page will be fed back as a blank page. The people in China can access their e-mail box, but they cannot read the e-mail content if this e-mail is so-called "sensitive." So, the people are waiting for some new technology to stop this kind of trouble.

Our project, called "Secure Email Proxy," is aimed for this purpose. Our mission is to provide a midway platform between the Chinese users within the firewall and the outside world.

The traditional way of encrypting information is to use software such as the popular PGP software. But the PGP software requires that both senders and receivers use the same software, so it limits the usage of such kind of software. Most e-mail senders in the United States do not use it because they do not need it. So, that could be a problem.

With our platform, we will forward all e-mail to Chinese e-mail users who are interested in our system. Our function is to encrypt normal e-mail, then to send it back to Chinese users. It will help Chinese Internet users to have secure e-mail communication with outside people who do not use encryption software such as PGP.

This will be very helpful. For example, in China, people subscribe to a mailing list from Voice of America, or Radio Free Asia. They can hardly receive the information, actually.

We think, with our help, they can subscribe to the mailing list and the information can come to us at the e-mail proxy server, and we will encrypt it and send it back to the real receiver. So, this will help them to skip the firewalls of the Internet gateway. That is the solution, and we are doing it.

That is all, thank you very much.

Mr. WOLF. Thank you very much.

Paul Baranowski.

STATEMENT OF PAUL BARANOWSKI, CHIEF ARCHITECT, PEEKABOOTY PROJECT, TORONTO, ON, CANADA

Mr. BARANOWSKI. Good afternoon. I am the project leader for Peekabooty, a piece of software that is designed to get around state-sponsored Internet censorship at the national level.

Peekabooty accomplishes this using peer-to-peer [PTP] technology. "Peer-to-peer" basically means that there is no central authority governing some part of the network system. The idea is that anyone using the peer-to-peer system also helps out other

people in the system at the same time. Napster, Gnutella, and others are all examples of peer-to-peer networks.

Peekabooty uses other nodes in the network to relay data around the firewall. It is kind of like a distributed proxy service.

China has been working on its firewall since at least 1997, and we have seen its power growing over the years. Just about every other month we are seeing a new technology being deployed that makes it even more powerful.

The Chinese authorities started blocking Web pages based on their Internet protocol addresses, which we have already talked about. People got around this initially by using open proxies, which are basically other computers that relay your requests for a Web page indirectly back to you.

In early 2001, the Chinese Communist Party countered the use of open proxies by scanning the Internet for them and adding these proxies to the ban list. Another thing that some Web sites did—apparently DynaWeb did as well—is that they changed their IP address every few days in order to try to prevent blocking of their Web site. But this is fairly ineffective.

Safe Web and Voice of America set up a system that would send the IP addresses of available proxies to whoever requested them. Again, DynaWeb also tried this technique. However, it was not long before the Chinese authorities started requesting the proxy addresses and blocking them as well.

There are two strategies that have not been effectively countered yet: bulk e-mail lists and freenet. Bulk e-mail still works because the origination of the e-mail is different every time. E-mail does, of course, has the drawback of being one-way communication, but at least that is something.

Freenet is a peer-to-peer system that allows two-way communication. It still works because the only way to discover a new node in the Freenet system is through "out-of-band" means. This means you have to call up a friend, or your friend has to e-mail you an IP address of another domain network. You join the network and then you can get access to censored information.

One of the main goals of Peekabooty is to eliminate this limitation, to create a method of discovery that automatically allows you to discover new nodes in the network without allowing you to discover all the nodes in the network, so that the Chinese authorities could not join the network and block everything.

Some of the 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 band key word. So, for example, if you search for Falun Gong on Google, your Internet access would be denied.

Suppressing dissident comments and chat rooms.—If you do type in some sort of dissident comments, a warning e-mail is sent to you telling you not to do that again.

Finally, they are starting to log Google key word searches. So if you type in "Falun Gong," they are going to remember who requested that.

We can do something about all of this if we act now. The Chinese Government is already on its third generation of firewall tech-

nology, and we have not even started version one of a counter-strategy yet. If we do not do something soon, they may be able to close off the country completely and obtain absolute control of their net before we can do anything about it.

A fair guess is that, by the Olympics in 2008, it will be much too late to act. Our window of opportunity is now, at this moment. The U.S. Government is the only organization that has the power to mount an effective counter against this type of censorship.

Independent efforts, such as mine, 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 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 inter-operation between the projects and allowing more advanced features in these projects, 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 type of activity on the scale that is required.

The amount of money proposed in the Global Internet Freedom Act could 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 here represents a sample of what is out there. There are perhaps a dozen grassroots efforts attempting to do something about this on a shoestring budget. They all rely on volunteers.

However, this many projects is not as many as we need. Right now, development on all of them is extremely slow, due to the fact that there is little funding and they all rely on volunteers.

The first thing that is dealing with funding, is development speed. The second thing, is usability. The third thing, is translation into various languages. Finally, every project that is funded should have a budget for marketing so that each project can be promoted appropriately.

If the 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 the fear of software back doors that would allow remote monitoring of or tampering with a user's computer.

Open-source software relieves these fears because the code can be vetted by outside experts. One of the most important things with many of the current projects, is that they use peer-to-peer technology. This means, in terms of costs, there is little cash that is needed to keep them running.

Funds are mainly needed for the maintenance of the code and the addition of new 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: Peekabooty, the Freenet/Freenet-China project, the Invisible IRC project, which allows anonymous chat, CryptoMail, which is a Web-based e-mail system similar to Yahoo which provides encryption of e-mail, and finally, plug-ins to e-mail clients such as PGP and GPG to make encryption of e-mail easier.

It should be noted that the National Science Foundation [NSF] has started funding anti-censorship research at the academic level. What we need, though, 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 type of technology could allow individual devices to route information on their own. This would allow those devices to bypass the Internet infrastructure completely and create basically a new wireless Internet that could not be filtered.

Also, another area of research that should be considered is making e-mail encryption even easier to use and more transparent. Right now, it is a little bit too difficult for most people.

Finally, to sum up, 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 instead of less.

Thank you.

[The prepared statement of Mr. Baranowski appears in the appendix.]

Mr. WOLF. Thank you very much.

Avi, you talked, first, about the arms race. You did not draw a conclusion. Is this arms race a winnable arms race on the circumvention side, or is it simply a continuing process of raising the costs at each level?

Mr. RUBIN. I, unfortunately, do not think there is a straightforward answer to that, because there are several different axes that I drew for censorship.

If you are talking about the censorship between the inside of China to sites that are outside of China, it is pretty clear where the end of the arms race is, which is that they cutoff all connectivity. Then, short of going through a satellite, or phone lines, or some other way, there is really no way anyone could get out.

However, there are a lot of other things. For example, if you look at people within China trying to communicate with other people within China, and maybe posting content where things are not going through the firewall, then I think there is an interesting arms race.

It is not clear who the winner is, because I think the technology has only advanced so far at present. We need new research. I support the comments that were made about funding new research.

You could imagine a technology developed whereby Internet traffic becomes untraceable, so the next thing that happens is that the government mandates router manufacturers to put something in each packet so that they can trace it. That is another step in the arms race. We have got to go back to the drawing table and figure out how to get around that, and I do not see where that kind of an arms race terminates.

Mr. WOLF. Anyone else want to comment on that?

Mr. XIA. I would.

Mr. WOLF. Yes, please.

Mr. XIA. I would like to make a little comment. Technically, you can comment on technology if it can be censored or it cannot, how hard it is.

Another factor is if the user will use it. Like, for the Freenet China project, there are people sending e-mails and saying, I am a peasant, I only went to elementary school, so tell me how to use it in two sentences, something like this.

So, even if technology works, there is the matter of, first, how can you overcome the first barrier, if you can convince the user to use the software and learn how to use it.

Mr. WOLF. Thank you.

Mr. BARANOWSKI. I have a comment.

Mr. WOLF. Go ahead.

Mr. BARANOWSKI. I think, if we do nothing, then eventually we will not be able to do anything. But if we do something soon, then the arms race will continue, and continue on indefinitely until whenever.

But there is a point that, if we do nothing now, we will not be able to do anything eventually because they would have cracked down too much at that point and there would be no way to get anything in or out.

Mr. WOLF. Is there a point in this arms race where the cost to China is too high, in the sense that the measures the government would have to take would so negatively impact on the use of the Internet, and on Chinese businesses' ability to use the Internet to be internationally competitive?

Mr. RUBIN. I think you have put your finger on it right there. If China were willing to isolate themselves from the rest of the world, then they could censor in a way that we probably could not overcome.

But as long as there are forces within China that want to have, for the sake of their own businesses, like you said, connectivity, then I think that there is something we can do.

I also see the door closing if nothing is done, but maybe not as fast. The thing that will push them to the next level in censoring is when circumvention technologies start to move. If they stagnate, then I do not see them having a need to respond.

Mr. XIA. I am also thinking of another possibility, that Western companies collaborate in doing censorship even outside of China. Then they can collaborate with censorship technology so it will not affect, like e-commerce communication, inside and outside of China. One technical example I can think of, is content filtering of any Web site—for example, Google—so if you are searching for key words, you are kicked out.

However, it is actually easy to resolve this. Google can just implement https so your requests will be encrypted. I am not sure if Google is willing to do that. It is obvious that Google will be confronting China's content filtering engine.

Mr. LIN. I might comment. I think those who do censorship and who did anti-censorship, they actually use similar technologies. The result is people or companies do something for profit. So that is why we see that the Chinese Government can create a firewall.

I think some U.S. companies are heavily involved with it, say, especially some companies in California. The backbone, the technology, and the core equipment are developed and manufactured by the United States, especially California companies.

So we do not have exact evidence, but we can reasonably conclude that the American companies are helping the Chinese Government to build the censorship firewalls. So that is why the same technology can result very differently for different sides. For people who are doing anti-censorship, like Paul, he is just doing it for the ideals, not for profit.

I think the two sides are not even. So, the result is, we can expect who will win the war. I do not think, in any small part, that we will win the war. That is the reality, so I am worried about it. So, I think it is my duty to speak here to help many people to understand the situation.

Mr. BARANOWSKI. Can I answer that as well?

Mr. WOLF. Sure.

Mr. BARANOWSKI. You raised a good point about the commerce and tying this anti-censorship technology to commerce. This is the only way I think that these technologies will work.

For example, using SSL [Secure Sockets Layer] encryption for secure communication. SSL is also used in e-commerce to buy things over the Web, so they cannot outlaw, for example, that type of encryption. So, this opens a whole lot of China which they cannot really block unless they want to block all of e-commerce.

The second thing I want to talk about is the stagnation of censorship technology that Avi mentioned. I do not think this would happen at all, because they are plowing forward as fast as they can to implement more and more technology. For example, the Golden Shield project. They are trying to use as much technology as possible to control their population. I do not think it is going to stagnate anytime soon.

Mr. WOLF. All right. Thanks.

Holly.

Ms. VINEYARD. I would like to follow up on Ira's point there. I would first direct this toward Paul. It is open for anyone else who would like to answer. As technologists, how would you characterize the economic cost of censorship?

I am interested in this as an approach for, how do we engage the Chinese to see the true economic potential of the Internet if it is left unfettered?

Mr. BARANOWSKI. Obviously it is costing them a lot of money to employ this many people to constantly be looking at Web sites and trying to filter them. So that's the obvious, up-front cost, as well as buying the right type of hardware equipment that they need.

Another economic cost that might be borne by them is the fact that they might be blocking sites that are not supposed to be blocked which are e-commerce sites, so if people cannot get to those sites, they will not be able to buy goods and services through those sites. That is just off the top of my head. Maybe someone else can answer that as well.

Mr. RUBIN. Well, I am not certain how much commerce there is from China to e-commerce sites in the United States, and I think that is something that should be looked at to figure out. That was used as a motivation for why they are not likely to block SSL, but blocking SSL is trivial. It is 443.

They just turn it off and say, we do not have SSL through our firewall. If it is not the case that people in China can purchase things on e-commerce sites in the United States, then that point is pretty meaningless. I do not know. Maybe somebody knows about that.

Ms. VINEYARD. Does anyone know if there is much in the way of e-commerce going the other way?

Mr. RUBIN. People in the United States purchasing things in China? I do not know, either. I would be surprised.

Mr. XIA. I do not think many people are buying things outside of China from inside China.

Mr. BARANOWSKI. Maybe not consumers, but maybe businesses. Of course, I do not think any of us have any data on this whatsoever. We are just making the best guesses that we can.

Mr. XIA. When China blocked Google, there was a big cry inside China and more people are complaining. They want to do research or just common activity and they are blocked.

Mr. BARANOWSKI. That is a good point. I believe it was businesses eventually that complained so much that Google was blocked that they had to unblock it.

Mr. WOLF. Let me just jump in here. Rather than e-commerce and individual e-commerce, as Chinese industry continues to develop and become more sophisticated, they are going to have global sourcing strategies that require fairly sophisticated use of the Internet, whether it is sourcing, inventory controls, and so on.

That is what I was getting at. Not so much individual e-commerce so much as, does additional effort by China to monitor, block, and control the Internet raise the costs, ultimately, of a joint venture auto manufacturer that is involved in global logistics?

Mr. RUBIN. Definitely. I mean, the way that I would envision that this would happen would be if they do not want to allow unfettered access to the SSL port, which someone serious about censoring would not because a lot of circumvention technologies could be built on it.

They could perhaps require any company or any entity that wants to do that to clear it with them, and then they would provide a special port and maybe some encryption keys that they know that they allow them to use, and then they could monitor it carefully. That would all be very expensive.

It would require a lot of databases to keep track of which keys are used for which communications, and then all of the monitoring equipment. So, they are raising the bar on themselves to some extent by making it more expensive to allow those business-type

communications that they want to allow while preventing general use.

Mr. XIA. I think this is true right now for e-mail service. If you are running e-mail service in China, you have to put in all the filtering software. For the Chinese ISPs, many of them have very sophisticated e-mail filtering software which will delay users receiving e-mails.

Also, many people will lose their e-mails. It is quite different from here. I can call you and say I just sent you an e-mail, but in China you cannot rely on this.

Ms. VINEYARD. Thank you.

Mr. FARRIS. I am wondering if any of you could speculate on what sort of attributes any anti-censorship or censorship circumvention software or project would have to have in order to be successful.

For example, I think issues like deniability on the user end, the receiver end, would be important. But perhaps Bill or Lin Hai can speak to whether or not they think that is really an important issue in China.

Other issues like user interface, I think you mentioned, or translations into Chinese. How important is it to the Chinese people at the user end that this be in the Chinese language, or does the average Internet user have an English level sufficient to use these programs? If any of you have any speculation on what a good censorship circumvention program would possess.

Mr. RUBIN. I can tell you what we did with Publius and some of the lessons that we learned in that regard. In terms of user interface, I think the best way to distribute client software is as a plug-in to a browser.

We experimented with client-side proxies. Those require someone who knows how to run a compiler in order to get them running, unless you want to write something native, but then people use many different operating systems.

The one common denominator seems to be a browser. So, a client-side plug-in would have the advantage of being able to have general-purpose functionality.

You could build your whole protocol into it, whatever that might be. Users would be able to not know necessarily exactly what it is doing and just have content displayed for them. So, as far as user interface goes, I think that is the way to do it.

That will not work in a cyber cafe, for example, where you do not have access to installing a plug-in. In that case, you need to go with raw html, and it is a lot harder because if you need to do any decryption or decoding or anything like that in the software, then the only way you might do that would be via a Java applet.

The Java applet would come from some well-known site, and that could easily be blocked. So, after looking at all the different alternatives, I think a browser plug-in is the way to go.

You mentioned deniability. In the Publius project, what we did was take the content that somebody wanted to publish and break it up into many, many little pieces. Those things had transformations performed on them so that you needed some subset of them to reconstruct the content.

So, here's an example. Take a piece of Web content, whether it is an image or a document, and break it up into 100 pieces such that any 4 of them can reconstruct it, but any fewer than 4 is meaningless and more than that is redundant. The idea here, is then you store those pieces on 100 different servers all over the world. We had a bunch of servers up and running in seven countries. This was a research prototype.

The sites that would host the content, they see this 1 piece out of 100 and they do not know what it is. So, there is deniability from the host server. Without three other pieces they do not know what it is and they do not necessarily have that information on where the other pieces are.

So it was a system for publishing something. It got dispersed throughout the Net. Nobody knew exactly what the individual pieces meant. Then somebody to retrieve it would get a special URL, or they could get a link through something, and by running a proxy on their machine that their browser talked to, could go out and get four pieces, do a cryptographic check-sum on them, verify that they had not changed, and then load the image into the browser or the document without the user having to be aware that all this happened behind closed doors.

Mr. BARANOWSKI. May I answer that as well?

Mr. WOLF. Please.

Mr. BARANOWSKI. As far as user interface, I think a variety of methods should be used depending on the individual user. Something different should be in an Internet cafe versus someone from a home computer, versus someone at a business, which is what I was getting at before in my speech. I was saying we should have multiple projects going on at once using a variety of methods.

As far as deniability, the only thing I can say is that this does exist in Peekabooty. The connections to the Web server are anonymous. No one can tell who is fetching which Web page.

As far as English level proficiency, I just read a report last week that said 20 percent of Web pages viewed from China are in English. So, definitely the minority. That is all.

Mr. LIN. May I comment? There are some informal technologies used by the Chinese Internet guys. They can always find some secret way to access the outside world. But the problem is, it is not public technology. So, the public needs to use most widely used technologies, say, for Web access.

I think if we can offset technology to let people use a normal browser to access the outside world, the effect or the result will be very limited. So, that is a problem. Not all people are educated in technology. They are just normal users.

Mr. XIA. I think the answer, a lot, depends on how many users you are targeting. For the most computer-capable people, many of them can read English. They will find ways themselves. They do not quite need your help. Like, DynaWeb has reached the level of tens of thousands. So at this level, you need something really easy. We got complaints, in the beginning, about DynaWeb using the domain name, or just visiting a Web site.

I cannot say anything easier than that. But, still, some people do not like the pop-up windows, https, because it is not certified, or something like that. Or we do some technology that makes the

domain name look weird, and then some users say, should I click it, or something like this.

So, even at this level of users there are lots of questions that arise. But if you are working on something like a plug-in or a program, people need to download a Chinese interface. That is important. Like for the Freenet China project, it has software and it reaches a user level of 10,000. So at this level of user base, you do need the Chinese interface, and a very easy-to-understand interface.

Another factor we tried to compile, is we want to put the program below 1.44 megabytes so people can carry it around with a floppy. Then people do not have to leave that program on their computer's hard drive, they can, every time, download it and delete it.

But this is getting harder because in the Internet cafe situation, it is really bad. In many of those registered Internet cafes, you cannot download and there is no floppy drive.

I think for some software, the administrator can remotely look at your screen at any moment. I think for this specific environment, it is almost like the door is closed. There is hardly anything to do with it.

Mr. RUBIN. Just one other point. In a country where it is illegal to do certain activity, you could conceive that if there were such a plug-in or proxy program, the fact that that thing is on your machine could be a liability.

Mr. FARRIS. So just a follow-up. In terms of the state-of-the-art right now, is it possible for there to be a system that has complete deniability, something that would not have to be downloaded, that would not involve any obvious encryption that would tip off the authorities?

Mr. RUBIN. It depends on your threat model. If you have a threat model that the authorities are sniffing your line, then the answer is, without encryption, no. If they do not allow encryption, then there is nothing you can do.

If you have authorities that are, with some probability, sniffing your line, then maybe you can play some games and adjust or tune your risk factor and say, I will get caught with this probability, and that may be able to be small enough that it would be worth it for people. But if the adversary can view the line going into your house and you do not allow encryption, then I do not see how there is anything you could do.

Mr. BARANOWSKI. Since China still does allow encryption, what you could do is if you are in China and you have a friend in the United States, you could download a program such as PGP Net, I believe, and encrypt all your data between the two computers, he sets it up on his computer and his computer is on all the time, and you just route everything through him.

So, it has to be more of a personal connection to someone who is going to help you out in another country, and then you could quite easily get around it. As far as an automatic system, there is no way right now to—sorry.

Could you repeat the question real quick?

Mr. FARRIS. I guess I am trying to see if it is possible to have complete deniability.

Mr. BARANOWSKI. Oh, complete deniability.

Mr. FARRIS. So nothing needs to be installed in the computer.

Mr. BARANOWSKI. Nothing that is automatic. Right.

Mr. FARRIS. Yes.

Mr. XIA. Technically, I think it is probably impossible to achieve that. But right now, I think the closest is DynaWeb. You only need a domain name to visit a Web site, and then you can clean your history with your Internet browser. But still, if someone is looking through your computer, still you can be caught.

Here, just now what Paul mentioned, I think, we can put in a social background.

Right now, downloading and using PTP will not get you into prison. But there are people arrested, and PTP is used as site evidence. So, just using PTP is fine, but if you are doing something else along with PTP then it is something else. I think this is an important point. In the last 20 years, China has changed a lot.

During the Cultural Revolution, all the requirements were really harsh. If you were listening to the VOA radio at midnight, you could be caught and sent to prison. But now the government, instead of arresting you, is only trying to jam VOA radio.

Mr. WOLF. Thanks.

Keith.

Mr. HAND. I wanted to get back to this arms race issue for a minute. I was curious what the typical timeframe is in terms of the cycle of technology and counter technology.

Then maybe you could follow it up with another point. There has been some concern expressed that, as these new technologies are developed, there could be a false sense of security among users in China as to the degree of protection that they have.

I was wondering if you could comment on that risk and whether, in your experience, people understand it or whether they feel like they are completely protected from monitoring when a new technology is introduced.

Mr. XIA. From my experience, they correct that mistake pretty quickly, like 1 day after. If they mistakenly block their own sites or something like that, they will correct that pretty quickly since they only need to release what they did with that technology. But to develop brand-new technology, from our recent experience, it is more like months. But for security concerns, I think you have to foresee it to be compromised.

Mr. RUBIN. To answer the other part of your question, it is interesting. When we came out with Publius, I got approached by somebody who wanted to use it for very sensitive—they did not tell me what—activities and they said they were really worried, and how much would I vouch for the software.

It is interesting, because normally if there is a bug in a program that I write, something crashes. But the responsibility of potentially putting someone in harm's way by a bug in the software was too much. So we disclaimed it and said, this is a research prototype. We did open-source it. I agree that open-source is an important component of anything like this.

If you are going to use a program that could get you thrown in jail if it does not behave properly, that is a pretty scary notion. I

mean, the way they measure the number of bugs in a program, the metric in software engineering, is by the number of lines of code.

You ask a software engineer, how many bugs does a program have, they say, well, how many lines of code? And then you know how many bugs it has, or a minimum, anyway.

So for something to be that reliable that you are going to risk your freedom to use it, I think it is tough and I am not sure that I would want to take that chance, myself.

Mr. HAND. Thank you.

Mr. WOLF. Paul, if you had a different hat, let us say as a representative of a U.S. intelligence agency, and you were sitting here as the fifth person on this panel, and you heard Paul Baranowski talk about the need to develop open-source software for countermeasures, what would you say to us in response?

Mr. BARANOWSKI. In response to what?

Mr. WOLF. Regarding the technology required for countermeasures, what concern would the intelligence community have that obviously bad people would put this to bad use?

Mr. RUBIN. The double-edged sword.

Mr. BARANOWSKI. Oh, yes. All right. I have been asked this question before. Yes, I would have concerns about whether bad people could use this technology for bad things. My response to that is I have tried to think of ways that, especially Peekabooty, could be used to do bad things and I am hard pressed to come up with something that is not already done better using the different programs specifically designed to do bad things.

There are plenty of programs out there in the Internet area that do bad things, like denial of service attacks, viruses. All this, you can get easily. So, something that simply makes your Web browsing anonymous, it is somewhat difficult to think of scenarios that you could use it to do evil with.

Mr. LIN. I might comment. I think no one can prevent some people from doing bad things with some technologies. So, based on this theory, to make any policy to limit people using technology, you will not really reach your goal.

For example, the PGP software. To my understanding, it is still banned for people outside of the United States to download the PGP software from U.S. Web sites. It is the United States law. So how do they do it? They just publish the PGP software, soft code, and carry it to Norway, and then retype it into the computer at the Web site in Norway at PGPI.com, or something like that.

So that other part of the world—outside of the United States—can download the same program. That is just an example. The United States making some kind of policy to try to limit the people using technology, it does not work. That is my opinion.

Mr. RUBIN. Getting back to your question for a minute, when Publius came out we took a lot of criticism from people who came up with the example, imagine somebody came up with child pornography or some other kind of offense-to-pretty-much-everybody image and posted it to a system where it was published where it could not easily be removed. That is something that was not possible before. Or instructions on how to make a bomb, or something like that.

You sort of take a step back when you suddenly think about uses of your technologies. There are several different ways to look at it. One is an example I go back to. When the automobile was first introduced, law enforcement was afraid to allow these things to be mass produced because they were worried bad guys would be able to get away more easily. Yet, we see all the good that has come out of the automobile. The same thing could be said for the Internet.

A more constructive answer, though, is to say that you can build censorship-resisting technologies with dials in them and let society set the dial. So in the United States, for example, we all believe pretty much—we should believe—in freedom of speech and the right to do certain things.

Then there are certain acts which pretty much are the norm in society that that is unacceptable, certain things like child pornography that there is just no debate about. So, perhaps we can build a censorship system so that if almost all the users in the system do not want something, then that thing can be censored, but it requires a communal effort of almost everybody. That is just some thoughts on how to do it. You have got to be very careful that you do not enable, accidentally, ways of censoring that are more easy than before.

Mr. WOLF. Let me turn to United States suppliers of technology, equipment and software for China's backbone. Lin Hai was talking about California companies. Others have talked about the need to license or restrict United States export of technology to China that can be used for censorship and control.

I wonder if you could comment on what you think should or could be done regarding control of United States exports of Internet technology to China, or whether it is something you believe is a road that we should not go down.

Mr. LIN. I think that it is not easy to make any kind of policy like that because people can find some ways, any ways, for profit. So my suggestion is, do some reverse policies to encourage companies, and individuals, and organizations to develop any other technologies against censorship. This is the way to work, I think. For example, set up some funds to sponsor people like Paul, to develop anti-censorship technologies. That is the right way.

Mr. BARANOWSKI. I would say to ask the companies themselves to have them issue a statement saying we do not support censorship and surveillance. We do not take part in it. For them to come out and publicly say that, I think, would be a very good first step in that process.

There is a precedent for regulating this type of technology, and that is with encryption. Just a few years ago, you had to first submit any encryption product to some agency to have it checked out before it was exported, so you could not export anything that encrypted above a certain level. This could also be done with censorship technology. That would be a more extreme thing to do, but there is precedent for it.

Mr. RUBIN. Yes. I pretty much would oppose any idea of regulating what Internet companies can and cannot sell abroad. While I agree with the goal, I think that such export restriction attempts have fallen flat on their face before, as we have seen with the encryption.

Mr. WOLF. Bill, do you have a comment on this?

Mr. XIA. I think it is kind of analogous to export arms so that arms can be used for good things or bad things. So, there can be restrictions on what kind of technology you can export and where you can export. They cannot just say, I am sending the technology, I do not know or I do not care what they are doing with it.

Especially for China, in the past years, it has been demonstrated, what are they going to do with content filtering technologies. So, I think there can be regulations on some specific cases.

Mr. RUBIN. I would worry that China would start buying their backbone technologies from other countries that have equally developed products, and that we would be hurting our business without actually helping fight censorship.

Mr. WOLF. Holly.

Ms. VINEYARD. If China has such effective cyber-walls, in your opinion, why is it these cyber-walls are not being used to stop piracy as well?

In the recent regulations, copyright piracy was not identified specifically as an illegal purpose. How do you recommend we go about raising this?

I mean, we would be asking the Chinese to provide additional policing to a medium that we essentially want to be free, but we still want to protect the rights of copyright holders.

Mr. XIA. I think Internet censorship has become a very essential policy of the Chinese Government. This year, the head of the Public Bureau of Security commented that there is a conspiracy about anti-China forces trying to distribute subversive information through the Internet.

I think for the Chinese Government, the Internet Freedom Act can potentially endanger their current authority, so it is a pretty high priority, not just economics.

Ms. VINEYARD. But my question was really trying to get at the protection of intellectual property rights, especially copyrighted material. If any of you have any experience with how that is being protected or not protected on the Chinese Internet, I would appreciate your views.

Mr. RUBIN. I think that it is really a different security technology that protects or prevents traffic from flowing freely and that guards intellectual property. It is almost like guarding the information in the other direction.

So, if something that is a particularly valuable intellectual property gets inside China and can get replicated very easily, the fact that it went through a firewall when it got through is meaningless at that point.

Intellectual property protection technologies are somewhat limited in their capabilities. If there is something that you have in software, you can replicate it. Hardware assistance is expensive. It is difficult to distribute things when you require people to have a particular kind of player.

Intel and Microsoft are taking steps to provide intellectual property protection in the platform that people have in their homes. At that point, if that works, it will be successful in China as well. But I do not think that the censorship technologies are designed, nor

can they very easily protect, intellectual property of something once it has gone through the firewall.

Mr. LIN. To my understanding, this is more consistent with the law. In China and in the United States, they seem to have similar copyright laws, but they actually deal with them very differently.

In China, on the big Web sites, they understand the copyright law, but individual users do not care. The government also does not care about the individuals who use free copies of copyrighted materials.

So, the censorship through technology will not help to protect the copyright, but it should be done by something like how to develop the law and how to actually do something under the law.

Mr. BARANOWSKI. Actually, one of the scary things is that if China does get this DRM technology, which is Digital Rights Management, which allows you to protect your intellectual property, if that goes to China, it actually gives China more power to censor their people because you could use that same technology to say, you can only run this program on your computer, or this set of programs on your computer, and nothing else that is not approved by the Chinese Government. Thus, no program that we could write, any anti-censorship program we could write, could ever bypass that sort of control.

Mr. RUBIN. And that is not limited to China. A lot of people worry that DRM technology in the United States could greatly restrict fair use of all kinds of things.

Ms. VINEYARD. Thank you.

Mr. FARRIS. I would like to stay on that point for a moment. I think at least Publius, and maybe also Peekabooty, were not specifically designed with China in mind, and there may be a concern about other countries as well.

Do any of you have a view on where China fits in the spectrum of censorship compared with, say, even the United States or other countries? Is China the worst offender? Do you see the United States moving in a similar direction?

Mr. BARANOWSKI. China is the worst offender, possibly tied with Saudi Arabia. The other countries that are censored are Burma, Cuba, and even Australia.

There are about 20 or 21 countries that censor their Internet the last time I checked.

You are right that this type of technology could work in any country. It is not just limited to China, which is, in my opinion, a good thing.

Mr. FARRIS. Thank you.

Mr. WOLF. Keith.

Mr. HAND. I wanted to get at Ira's question from a slightly different angle. There was a lot of controversy over the Yahoo China pledge earlier this year. Some argued that even operating under some restrictions, there is still an advantage to having a company like Yahoo operating in China, delivering information and pushing the limits of the controls there where they can.

I was wondering if you could comment on that and give us your sense of where you think the line should be drawn between working within the system and struggling within it for change, and

where you end up colluding with the government on these censorship issues.

Mr. RUBIN. I think that anything that encourages the openness, the connectivity between China and the rest of the world, opens up avenues for other censorship-defeating technologies to piggy-back on the existence of that network. So, from that sense I think it is a good thing.

Mr. BARANOWSKI. It seems to me that companies going into China are playing right into their hands. China basically stops any company from coming in unless they obey their rules.

So, basically it does not seem like any Western thought is getting into China through these corporations. For example, the Norton Antivirus software. They gave China virus software before they could get into China. Cisco built special routers for them.

All these companies are playing right into their hands and basically doing whatever the Chinese Government says so they can get into this imaginary market, in my opinion, that is not quite as big as they made it out to be.

Mr. XIA. I agree with what Paul said, especially in the case of Yahoo. They have openly signed a self-censorship agreement. In the case of Yahoo, it actually helped China to create a kind of Chinese Internet and make it look like people can stay there and get everything.

Mr. WOLF. Paul, you just said Cisco provided special routers. Are you saying that the Chinese Internet censors provided specifications to Cisco to provide some unique equipment, or are we talking about equipment that they provided that have multiple uses?

Mr. BARANOWSKI. The reports are that they asked for specific features in these routers, and Cisco made it for them.

Mr. WOLF. Is it your assumption that those features are unique?

Mr. BARANOWSKI. Unique to China.

Mr. WOLF. Unique to censorship functionality as compared to some other functionality?

Mr. BARANOWSKI. To censorship technology.

Mr. WOLF. But that is a guess, right?

Mr. BARANOWSKI. These are reports from interviews of people that worked on the project, so I do not have direct experience with that.

Mr. WOLF. As you develop circumvention technologies, is the target user the average Internet user in China, or is the target someone who has a fair amount of sophisticated knowledge? In other words, is the beneficiary someone who has a PC at home, does not know much about the technology but knows how to sign onto his ISP?

Mr. BARANOWSKI. Are you saying, for Peekabooty, is that the main target market?

Mr. WOLF. Yes.

Mr. BARANOWSKI. Yes. Yes. For my project, Peekabooty, that is the target market, the personal home computer or any computer you can actually install software on.

Mr. WOLF. And a user who is not particularly sophisticated.

Mr. BARANOWSKI. Yes, and a user that has no special knowledge of Internet technology.

Mr. WOLF. Avi.

Mr. RUBIN. Since it was a research prototype, we never got it to that phase. But the design was made with that as one of the original main constraints, is that it should be usable by anyone.

Mr. WOLF. Bill.

Mr. XIA. From the response I got, there are people who really have little computer technology. They ask me, you gave me the URL. What should I do? So I have to tell them, please copy the URL to the address of your Internet browser and return. You will see the Web interface, blah, blah, blah.

Mr. WOLF. All right.

Mr. LIN. I think nobody can get benefits from a virus. If the government, for some purpose, makes some special virus that is very dangerous and powerful, you can understand because most of the users are uneducated in special technology. They will not find anything special.

All information can be collected by the central government. It is very easy and effective and could happen. We have not had any reports that it has already happened, but it is just a technical possibility.

Mr. RUBIN. It is actually pretty bad. There is a program out there for Windows, which is the most popular platform, called Back Orifice. It is a spoof on the name Back Office.

What this program does, is it can be installed on a computer in stealth mode, meaning that you cannot really tell that it is running on your computer, and it provides a remote terminal to whoever installed it there where they would have a window on their screen that was exactly your desktop, whatever you saw there.

They could control it with mouse clicks and keyboard events that would be sent from their computer to the target computer, and anything that was done on that target computer would be visible, and any keystroke, any password that was typed in, would be visible.

So in the extreme where the government wishes to install this kind of a virus, or even to require vendors to install this on the computer when they sell them, they could pretty much see exactly what was going on on every single computer any time they wanted. Big brother. Turn the switch on this house and watch what is going on on that computer. That is not just technically feasible, that has already been done. That software is out there.

Mr. WOLF. I have one last question. Bill, the figure of 30,000 Internet police. Where does that come from?

Mr. XIA. I think it is originally from some report from China, and then everybody is quoting it.

Mr. LIN. There is a specific Web site. They publish a lot of information related to the Web site, at dfn.org, Digital Freedom Network. That is my recommendation. You can find some information related to it.

Mr. WOLF. All right. Well, I would like to thank you all very much for coming today. This has been helpful in our understanding of the Internet technology issues. I appreciate the fact that, although you are all technologists, you talk about it in a way that non-technologists can understand.

So, thank you all very much for spending the time, and thank you all for your commitment to this.

[Whereupon, at 4:13 p.m. the roundtable was concluded.]

A P P E N D I X

PREPARED STATEMENTS

PREPARED STATEMENT OF AVI RUBIN

NOVEMBER 4, 2002

While I am a researcher at AT&T Labs, I am participating in this round table as an individual, representing only my personal beliefs and opinions. I have been researching computer security issues since 1991. Much of my work has focused on privacy, anonymity, and censorship resistance.

The purpose of my statement is to discuss technical issues related to censorship. I will discuss the techniques that a network administrator, including a large company or a country, could use to censor access and content to and from its network, and I will discuss techniques that could be used to circumvent this censorship. For the remainder of this paper, I will refer to the party controlling the network as the Censor, and to the party wishing to circumvent censorship as the User.

Censorship is somewhat of a broad term. It can refer to the blocking of access to web sites. It can refer to blocking all connectivity outside of the domain of the Censor, and censorship can refer to the limitation of access to certain content. Censorship can also involve forceful removal of content from the Web, by applying pressure to the publisher and/or the web hosting party. The latter is the type of censorship that the Publius system was designed to circumvent. In this statement, I do not discuss censorship within the domain of the Censor, but rather, the censorship of content available from outside of the domain for people whose network is under the control of the Censor. I also focus on the User as the receiving party of information and not the publishing party. I will be happy to discuss issues related to the latter in the question and answer period.

There are three principle techniques that can be employed by the Censor.

1. *Routing filters:* The Censor is in a position to control how traffic from the User reaches the rest of the Internet. The Censor can refuse to route Internet packets from the User that are destined for particular locations. Thus, the Censor can use the destination address of the packets to make a censorship decision. In the extreme, the Censor can prevent all traffic from all of its users from reaching any network outside of its control. This is easy to do, and any Censor can accomplish this without the need to purchase any new hardware or software. The functionality is built into all off the shelf routing equipment that sites use to connect to the Internet.

2. *DNS tricks:* The Censor can exert some control on which external sites users can communicate with by virtue of its control over the Domain Name Servers (DNS) within its administrative boundary. The DNS is the service that maps computer addresses (IP addresses) to names. For example, wow.avirubin.com has the address 207.140.168.155. Computers communicate using such numerical address, but people enter readable names into web browsers. The DNS translates these names into numbers. Since the Censor controls its own DNS service, it can translate requests from the User to addresses under its own control. For example, if the User attempts to connect to www.avirubin.com, the Censor can program its DNS to return 10.10.32.1 when the User's machine tries to figure out the IP address of the machine, and this address can be that of a machine controlled by the Censor. Thus, DNS provides the Censor with the ability to control which computers the User can connect to.

3. *Application level filtering:* The previous censorship techniques dealt specifically with connectivity issues. Application level filtering, on the other hand, is a mechanism for controlling the content, even if the User can connect to a server. The most likely type of application level filter that the Censor would use is an HTTP proxy. This is a program that intercepts requests sent to Web servers and the responses returned to the User. The Censor can inspect the content, and a decision can be made, as to whether or not to block the information from reaching the User. A Censor using an HTTP proxy might focus its attention on popular search engines.

The first type of censorship, based on routing filters, is difficult to circumvent. If the routers do not allow packets in and out of the network, then there is no way to get around that. The best one could do is to dial up to an external ISP. Of course, this could get expensive if the Censor is a country. Also, a very strict and powerful censor could monitor the phone network for data dial-up connections and disconnect them, as well as sanction the User.

The second type of censorship, based on DNS spoofing, can be circumvented by users who know the IP address of the server with which they wish to communicate.

Instead of referring to the server by name, they could connect using the IP address directly. However, IP addresses change frequently, and it may not always be possible for users under the control of the Censor to know the IP address of a server. In general, this is not a very effective technique.

The third type of censorship, based on application level filtering, is perhaps the easiest to circumvent. Encrypted content is difficult to censor, but a very strict Censor can maintain a policy of blocking all content that it cannot interpret for the purposes of filtering. Perhaps the easiest way to bypass HTTP proxies is to proxy web content over a different port. Port numbers are used on the Internet to identify the type of service for packets between hosts. For example, Web traffic uses port 80. HTTP proxies process packets that are marked with port 80. A User wishing to circumvent this monitoring could cooperate with someone on the outside of the Censor's administrative control. They could set up two proxies. The inside one would translate port 80 packets into ones that use, say, port 14500. The outside one would translate port 14500 back to port 80 and send them to the server. Thus, the User could browse the Web without the Censor detecting it. However, a strict censor could block all ports except 80, and then filter on port 80. There is little that could be done by the User in that case. It should be noted that researchers have succeeded in identifying services by their traffic patterns, independent of port numbers.

The bottom line is that there is an arms race in censorship. An extreme Censor can win every time, but at the expense of completely disconnecting all users. The more tolerant a Censor, the more avenues there will be for circumvention of the censorship that is in place.

PREPARED STATEMENT OF BILL XIA

NOVEMBER 4, 2002

DynaWeb was launched on March 12, 2002. It is a proxy network that allows users to circumvent the Internet censorship in China and to have secure and full access to the Internet. Users use DynaWeb as an information web portal to all other web sites. Since the inception of DynaWeb, we have managed to stay ahead of the censorship by China most of the time. 20,000 unique users gained regular unblocked access to the Internet through us.

DynaWeb has already played several rounds of the censorship and anti-censorship game in the past 8 months.

Before I start, I would like to explain a few critical technical terms for understanding DynaWeb experience. There are two ways to access a web site through an Internet browser. One is to type in the domain name, for example, www.google.com. The other way is to type in the IP address of the domain name. The IP address is the essential place the browser will fetch the web site information for the user. However, domain name is more user-friendly. After a user types in a domain name, web browser will resolve domain names to IP addresses and fetch the right information for the user.

The game started with e-mail subscription service. DynaWeb e-mailed unblocked IP address updates to subscribers. After 2 weeks, the censors probably subscribed to our e-mail service too because the valid time window of DynaWeb IP addresses reduced to a range from a couple of hours to a few days after release.

Then our services expanded to domain names with dynamic IP addresses. However, censors started chasing DynaWeb domain by automatically detecting the IP addresses that pointed to the domain name. This dramatically increased the needs for back-up IP addresses, hence increased the cost of DynaWeb maintenance. DynaWeb adopted new strategy so that censors had to manually verify the IP addresses before blocking it. Then automatic IP blockage stopped.

Soon in August, users started to have difficulty of accessing DynaWeb through https even the IP was not blocked. It was found out later on that the certificate DynaWeb used for secured access from the Internet browser was filtered. This can be achieved by package level analysis of Internet traffic to find out signature related to the certificate DynaWeb used. In response to this, DynaWeb started to change its certificate daily. No reports of certificate blocking have been found since then. Again, censors were frustrated with the resource required for daily updates of all related content filtering engine, and quit.

At the end of September, DynaWeb domain names were hijacked to a fixed IP 64.33.88.161 in China, along with many other web sites like www.voa.gov. DIT has published a detailed report about this hijacking (http://www.dit-inc.us/report/hj.htm), and it can be independently verified from the U.S. More study about this hijacking is still undergoing and will be released after we pass this stage.

So, what is next with the Cyber-wall?

At the first look, it is a technical question if technology can break through China's Cyber-wall. In fact it is not. This process is a race of technology and time. As DynaWeb's experience has demonstrated, both parties can always implement new technologies to stay ahead and sustain the advantage. If Internet breakthrough is defined as a pure technical issue, the future is brighter for censors because China purchases the most advanced censorship technology from western companies.

China is also developing the Golden Shield project, a "data base-driven remote surveillance system." When the whole Beijing city is wired with biometric sensor and camera network, no Internet based anti-censorship can get around the surveillance system.

Even now, during the 8 months of technical race with DynaWeb, China has developed the largest and most sophisticated IP blocking and content filtering system in the world. The more anti-censorship technique is deployed, the more comprehensive censorship technology has become. This leaves less and less technical room for anti-censorship. It is critical to take full use of technologies to benefit as many people as possible before the door is closed.

Second, it is a matter of available resources. China has 30,000 Internet police specialized on Internet censorship, and ISPs are forced to perform self-censorship. The self-censorship is even adopted by foreign ISPs such as Yahoo. China has purchased top technology from western companies. These technologies have even been modified for China's particular censorship needs. Nortel, Sun Microsystems, Cisco and many smaller companies contributed to building China's Cyber-wall.[1]

Comparing to China's investment in censorship and cyber wall, investment in breaking through this Cyber-wall is next to nothing. There are very few groups developing technologies suitable for this Wall. With more resources, DynaWeb can provide services to more people, develop better client software, have closer monitoring of censors' new technologies and respond faster.

Third, people develop technology and technology serves people. People factor is the most important factor eventually. Recent increase of public awareness about China's Internet censorship both inside and outside of China is a great sign. We hope that this will help improve the current situation soon. Currently companies contributing to China's Cyber-wall bear little public pressure, not mention any legislative limitation.

Inside China, more and more harassment and arrests of dissidents and journalists are related to the Internet. Last year, there are more than ten arrests in China for distributing forbidden information. This will create fear among the public. For the general public in China, they are now gradually realizing the existence of censorship consciously.

More importantly, government has adopted subtler mind control and propaganda to decrease Chinese's interests in uncensored information. All major events outside of China are reported, with seemingly a variety of views, although all the different views are in fact the government's view. There is a fully developed online community inside China serviced by self-censoring ISPs. This strategy is an extension of China's Cyber-wall, a wall in people's mind. Internet, combined with TV, newspaper and other information channels now offers Chinese people different types of information and different views on certain issues. It looks like that full freedom of speech has been achieved. However, the government produces all the different views and types of information. The censors try to use this to reduce people's interest in uncensored information.

In summary, technology along won't decide the future of China's Cyber-wall. But people do. If all Chinese people would like to obtain uncensored information, the Cyber-wall will be broken, from the inside.

---

[1] China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China, by Greg Walton, International Centre for Human Rights and Democratic Development http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html

PREPARED STATEMENT OF PAUL BARANOWSKI

NOVEMBER 4, 2002

I am the project leader of Peekabooty, a piece of software that is designed to get around state-sponsored Internet censorship at the national level. Peekabooty 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. Peekabooty 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 Peekabooty 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 U.S. 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 U.S. 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: Peekabooty, 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.