The New York Times

NEW YORK, WEDNESDAY, JANUARY 13, 2010

GOOGLE MAY END VENTURE IN CHINA OVER CENSORSHIP

REVERSAL OF PRACTICES

Company Says Activists' E-Mail Accounts Were Targets

*This article was reported by **Andrew Jacobs, Miguel Helft** and **John Markoff** and written by Mr. Jacobs.*

BEIJING — Google said Tuesday that it would stop cooperating with Chinese Internet censorship and consider shutting down its operations in the country altogether, citing assaults from hackers on its computer systems and China's attempts to "limit free speech on the Web."

The move, if followed through, would be a highly unusual rebuke of China by one of the largest and most admired technology companies, which had for years coveted China's 300 million Web users.

Since arriving here in 2006 under an arrangement with the government that purged its Chinese search results of banned topics, Google has come under fire for abetting a system that increasingly restricts what citizens can read online.

Google linked its decision to sophisticated cyberattacks on its computer systems that it suspected originated in China and that were aimed, at least in part, at the Gmail user accounts of Chinese human rights activists.

Those attacks, which Google said took place last week, were directed at some 34 companies or entities, most of them in Silicon Valley, California, according to people with knowledge of Google's investigation into the matter. The attackers may have succeeded in penetrating elaborate computer security systems and obtaining crucial corporate data and software source codes,

Continued on Page A3

From Page A1

though Google said it did not itself suffer losses of that kind.

While the scope of the hacking and the motivations and identities of the hackers remained uncertain, Google's response amounted to an unambiguous repudiation of its own five-year courtship of the vast China market, which most major multinational companies consider crucial to their growth prospects. It is also likely to enrage the Chinese authorities, who deny that they censor the Internet and are accustomed to having major foreign companies adapt their practices to Chinese norms.

The company said it would try to negotiate a new arrangement to provide uncensored results on its search site, google.cn. But that is a highly unlikely prospect in a country that has the most sweeping Web filtering system in the world. Google said it would otherwise cease to run google.cn and would consider shutting its offices in China, where it employs some 700 people, many of them highly compensated software engineers, and has an estimated $300 million in annual revenue.

Google executives declined to discuss in detail their reasons for overturning their China strategy. But despite a costly investment, the company has a much smaller share of the search market here than it does in other major markets, commanding only about one in three searches by Chinese. The leader in searches, Baidu, is a Chinese-run company that enjoys a close relationship with the government.

Google executives have privately fretted for years that the company's decision to censor the search results on google.cn, to filter out topics banned by Chinese censors, was out of sync with the company's official motto, "Don't be evil."

"We have decided we are no longer willing to continue censoring our results on google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all," David Drummond, senior vice president for corporate development and the chief legal officer, said in a statement.

Wenqi Gao, a spokesman for the Chinese Consulate in New York, said he did not see any problems with google.cn. "I want to reaffirm that China is committed to protecting the legitimate rights and interests of foreign companies in our country," he said in a phone interview.

In China, search requests that include words like "Tiananmen Square massacre" or "Dalai Lama" come up blank. In recent months, the government has also blocked YouTube, Google's video-sharing service.

While Google's business in China is now small, analysts say that the country could soon become one of the most lucrative Internet and mobile markets, and a withdrawal would significantly reduce Google's long-term growth.

"The consequences of not playing the China market could be very big for any company, but particularly for an Internet company that makes its money from advertising," said David B. Yoffie, a Harvard Business School professor. Mr. Yoffie said advertising played an even bigger role in the Internet in China than it did in the United States. At the time of its arrival, the company said that it believed that the benefits of its presence in China outweighed the downside of being forced to censor some search results here, as it would provide more information and openness to Chinese citizens. The company, however, has repeatedly said that it would monitor restrictions in China.

Google's announcement Tuesday drew praise from free speech and human rights advocates, many of whom had criticized the company in the past over its decision to enter the Chinese market despite censorship requirements.

"I think it's both the right move and a brilliant one," said Jonathan Zittrain, a legal scholar at Harvard's Berkman Center for Internet and Society.

Rebecca MacKinnon, a fellow at the Open Space Institute and an expert on the Chinese Internet, said that Google had endured repeated harassment in recent months and that by having operations in China it potentially risked the security of its users in China. She said many Chinese dissidents used Gmail because its servers are hosted overseas and that it offered extra encryption.

"Unless they turn themselves into a Chinese company, Google could not win," she said. "The company has clearly put its foot down and said enough is enough."

In the past year, Google has been increasingly constricted by the Chinese government. In June, after briefly blocking access nationwide to its main search engine and other services like Gmail, the government forced the company to disable a function that lets the search engine suggest terms. At the time, the government said it was simply seeking to remove pornographic material from the company's search engine results.

Some company executives suggested then that the campaign was a concerted effort to stain Google's image. Since its entry into China, the company has steadily lost market share to Baidu.

Google called the attacks highly sophisticated. In the past, such electronic intrusions have either exploited the practice of "phishing," to persuade unsuspecting users to allow their computers to be compromised, or exploited vulnerabilities in software programs permitting the attacks to gain control of systems remotely. Once they have taken over a target computer, it is possible to search for specific documents.

People familiar with the investigation into the attacks said they were aimed at source code repositories at high-tech companies. Source code is the original programmer's instructions used to develop software programs and can provide both economic advantages as well as insight into potential security vulnerabilities.

In its public statement Google pointed to a United States government report prepared by the United States-China Economic and Security Review Commission in October and an investigation by Canadian researchers that revealed a vast electronic spying operation last March.

The Canadian researchers discovered that digital documents had been stolen via the Internet from hundreds of government and private organizations around the world from computer systems based in China.

ELIZABETH DALZIEL/ASSOCIATED PRESS

Google's offices in Beijing, in April 2007. The company said Tuesday that it would consider ending its operations in China.

Andrew Jacobs reported from Beijing, and Miguel Helft and John Markoff from San Francisco. David Barboza contributed reporting from Shanghai, and Jonathan Ansfield from Beijing.

Business Day
The New York Times
THURSDAY, JANUARY 14, 2010

Google Is Not Alone in Discontent, But Its Threat Stands Out

By KEITH BRADSHER and DAVID BARBOZA

HONG KONG — Google is far from alone among Western companies in its growing unhappiness with Chinese government policies, although it is highly unusual in threatening to pull out of the country entirely in protest.

Western companies contend that they face a lengthening list of obstacles to doing business in China, including "buy Chinese" government procurement policies, widespread counterfeiting and growing restrictions on foreign investments.

Some of these obstacles are a result of China's desire to maintain control over internal dissent. Others stem from China's efforts to become internationally competitive in as many industries as possible.

Google's difficulties and its strong response are indicative of a broader shift in sentiment among multinational executives in China.

"I have never seen the foreign business sentiment as pessimistic as it is right now," said James McGregor, a consultant in Beijing. "There's a sense China is saying, 'We have your technology and your capital — and now we have control of the market.'"

Google complained on Tuesday about attacks on its computers that it said

Continued on Page 4

From First Business Page

originated in China and said it was no longer willing to censor its Chinese site's search results. It is not the first company to run afoul of the Chinese Communist Party's fears of social instability and strong desire to keep tabs on dissidents and limit freedom of expression.

China has long restricted the sale of foreign movies, books, music and other media and continues to do so while appealing a World Trade Organization ruling in August that these policies violate China's legally binding commitments to the international free trade system. More recently, China has sought to strengthen its domestic encryption industry — for which the government has easy access to all the decryption codes — while withholding the government certification that foreign-owned encryption companies in China need to sell their products to many users.

Jörg Wuttke, the president of the European Union Chamber of Commerce in China, said that no European Union companies had pulled out of China yet. But he said the encryption dispute would be the most likely cause if any European company withdrew in the near future.

Duncan Clark, the chairman of BDA, a consulting firm in Beijing that advises major telecom and technology companies, said that Google's difficulties were indicative of broader troubles for foreign companies in China.

"There has been a raft of decisions and unpredictability, a kind of unpleasantness about what's happening here," Mr. Clark said. "There has been this received wisdom that no one can afford not to be in China, but that is being questioned now — there's kind of an arrogance that's characterizing government policy toward multinationals."

To be sure, doing business in China has never been easy. Foreign companies have long complained of being cheated by joint venture partners who set up parallel businesses on the side or abscond with assets. Many other countries also have policies that favor homegrown companies, although the opportunity for industrialized countries to do so is limited because they operate under tighter World Trade Organization rules than China.

Chinese officials and academics dispute whether government policies are discriminatory toward foreign companies. Hu Yong, an associate professor of journalism and communication at Peking University, said that the government was leery of the rapid expansion of the Internet and mistrustful of private Chinese companies as well as foreign businesses.

"I think in the information technology sector, not only foreign companies are under very heavy pressure, but also private domestic companies," he said. "The general trend is that the government wants state-owned companies to occupy major positions in this field."

Other strains between China and the West over business matters have grown out of government policies that shield Chinese companies from international competition. These policies allow companies to grow in a large home market and prepare to export to less-protected markets abroad.

The newest frictions, particularly in the last year, have been over government procurement policy. When China joined the W.T.O. in November 2001, it promised to negotiate as quickly as possible to join the organization's side agreement requiring free trade in government buying. But it has never actually done so, leaving the Chinese government free to use its enormous buying power to steer contracts to Chinese-owned companies.

The National Development and Reform Commission, China's top economic planning agency, ordered national, provincial and local government agencies on June 4 to buy only Chinese-made products as part of the country's nearly $600 billion economic stimulus program; imports were allowed only when no suitable Chinese products were available.

China has also restricted exports of a long list of minerals for which it mines much of the world's supply, like zinc for making galvanized steel and so-called rare earth elements for manufacturing hybrid gasoline-electric cars.

Those restrictions, ranging from steep export tariffs to tonnage quotas and even export bans, have made it cheaper for many manufacturers to locate their factories in China to make sure that they have a plentiful supply of raw materials free from export taxes. In June, the United States and the European Union filed a W.T.O. case challenging China's restrictions on zinc and bauxite exports. The Chinese government has denied wrongdoing.

JASON LEE/REUTERS

A woman examined bouquets and messages left by Google users on Wednesday outside the Internet search company's headquarters in Beijing.

China's weak protections for patents and trademarks — and widespread counterfeiting as a result — have produced large industries that make goods in direct competition with Western competitors, but without comparable spending on research or marketing. Many Western companies have tried to respond by limiting the intellectual property that they transfer to China.

Oded Shenkar, a professor of business management at Ohio State University and author of "The Chinese Century," said very few companies would be willing to leave a market as big as China's, and that it might make sense only for a company like Google whose primacy rested almost entirely on intellectual property.

"The U.S. is the world's greatest innovator and China is the world's greatest imitator," Mr. Shenkar said. "Google? What do they have other than intellectual property? If by being in China you're at risk of losing it, maybe you don't want to be there."

But the Chinese market is so large and competitive that many multinationals choose to offer their latest technology for fear of losing market share if they don't.

Volkswagen used dated technology in the cars that it sold here in the 1980s and 1990s, so the Chinese government asked multinational automakers in the mid-1990s which of them would offer the most advanced technology in exchange for the right to enter the market and build a factory in Shanghai. General Motors won the contest and brought its latest robots and automotive designs to China in a joint venture with Shanghai Automotive.

China has become the world's largest auto market, yet it still limits foreign automakers to 50 percent stakes in auto assembly plants in China and assesses steep tariffs on imported cars. Chinese automakers that formed joint ventures with multinationals, like First Auto Works and Shanghai Automotive, have grown into giants that are now beginning to produce their own models, designed and built almost entirely in China.

The Chinese government has been introducing similar policies to force international companies to transfer their best technology in a long list of industries, like railroad locomotive manufacturing and aircraft assembly. It has also tried to give market preferences to domestic companies that invest in developing their own technology, even if the homegrown technology is initially inferior to foreign technology.

In November, the Chinese government notified domestic and foreign companies alike that the government would give preference in its purchases to products that used technology developed in China and had trademarks that were registered first in China. That led to a strong letter of protest by 34 industry associations to China's Ministry of Commerce.

Mr. McGregor suggested that Google's decision might prove to be a turning point.

"This may be seen as a real watershed," he said. "There is a lot of feeling that the U.S. is on a downward spiral and China is on the rise."

The New York Times

NEW YORK, THURSDAY, JANUARY 14, 2010

In Google's Rebuke of China, Focus Falls on Cybersecurity

Concerns Could Force White House to Weigh In

By MIGUEL HELFT and JOHN MARKOFF

SAN FRANCISCO — Even before Google threatened to pull out of China in response to an attack on its computer systems, the company was notifying activists whose e-mail accounts might have been compromised by hackers.

In a world where vast amounts of personal information stored online can quickly reveal a network of friends and associates, Google's move to protect individuals from government surveillance required quick action. In early January, Tenzin Seldon, a 20-year-old Stanford student and Tibetan activist, was told by university officials to contact Google because her Gmail account had been hacked.

Ms. Seldon, the Indian-born daughter of Tibetan refugees, said she immediately contacted David Drummond, Google's chief legal officer.

"David informed me that my account was hacked by someone in China," Ms. Seldon said in a telephone interview. "They were concerned and asked whether they could see my laptop."

Ms. Seldon immediately changed her password and became more careful of what she wrote. She also allowed Google to examine her personal computer at the company's request. Google returned it this week, saying that while no viruses or malware had been detected, her account had indeed been entered surreptitiously.

Google confirmed Ms. Seldon's account of events, but declined to say whether it had notified other activists who might have been victims of hacking.

Mr. Drummond said that an attack originating in China was aimed at its corporate infrastructure.

While the full scope of the attacks on Google and several dozen other companies remains unclear, the events set off immediate alarms in Washington, where the Obama administration has previously expressed concern about international computer security and attacks on Western companies.

Neither the sequence of events leading to Google's decision nor the company's ultimate goal in rebuking China is fully understood. But this was not the first time that the company had considered withdrawing from China, according to a former company executive. It had clashed repeatedly with Chinese officials over censorship demands, the executive said.

Google said on Tuesday that that in its investigation of the attacks on corporations, it found that the Gmail accounts of Chinese and Tibetan activists, like Ms. Seldon, had been compromised in separate attacks involving phishing and spyware.

Independent security researchers said that at least 34 corporations had been targets of

Continued on Page A12

From Page A1

the attacks originating in China.

Adobe, a software maker, said it had been the victim of an attack, but said that it did not know if it was linked to the hacking of Google. Some reports suggested that Yahoo had been a victim, but a person with knowledge said that Yahoo did not think that it been subject to the same attack as Google.

The decision by Google to draw a line and threaten to end its business operations in China brought attention to reports of Chinese high-technology espionage stretching back at least a decade. But despite Google's suggestion that the hacking came from within China, it remained unclear who was responsible. Nevertheless, it presented the Obama administration with a problem of how to respond.

Google's description of the attacks closely matches a vast surveillance system called Ghostnet that was reported in March by a group of Canadian researchers based at the Munk Center for International Studies at the University of Toronto. They found that an automated espionage system based in China was using targeted e-mail messages to compromise thousands of computers in hundreds of governmental organizations. In each case, after the computers were controlled by the attackers, they were able to scan for documents that were then stolen and transferred to a digital storage facility in China.

Some are told their accounts may have been compromised.

The researchers stopped short of directly accusing the Chinese government of masterminding the attacks. However, for years there have been reports of attacks planned by so-called patriotic hackers in China, and many American security specialists argue that these are simply irregular elements of the People's Liberation Army. At the same time, hackers frequently use so-called false flag espionage or denial of service attacks to route their activities through the computers of a third country and hide their identity.

One of the Canadian researchers said that fellow computer security researchers suspected that the attack on Google and other recent intrusions relied on hackers sending booby-trapped documents that were stored in Adobe's Acrobat Reader format, which then infect victims' computers. This method was seen in a recent wave of attacks on the Dalai Lama's computers. "We've seen a huge upsurge in attacks using Adobe Acrobat," said Greg Walton, an editor at Information Warfare Monitor, a publication of the Canadian research group.

A spokeswoman for Adobe said the company was investigating the reports, but could not confirm that the Adobe software was linked to the most recent attacks.

For Google, the attacks appeared to have been the final straw in a series of confrontations with Chinese authorities.

Top Google executives, including the chief executive, Eric E. Schmidt, and the co-founders, Larry Page and Sergey Brin, were ambivalent about the decision to go into China in 2006, which involved agreeing to censor some search results on the company's local search engine, according to a former executive with knowledge of the discussions. The resistance was strong from Mr. Brin, who had grown up in the Soviet Union.

But after discussions and internal lobbying from Chinese and Chinese-American employees inside Google, as well as some of the company's sales executives, Google's top executives came around. They were particularly swayed by the argument that even a censored version of Google's search engine would provide Chinese people more access to information and help promote free expression in that country.

Once the decision was made, however, Google began expanding its operation in China, which it expected would grow to be one of the largest Internet markets.

Ashlee Vance contributed reporting from Mountain View, Calif., and Thom Shanker from Washington.

During Mr. Schmidt's 2006 visit to China, shortly after Google introduced the company's China-based search engine, Google.cn, he told reporters that it would be "arrogant" to try to change China's censorship laws.

But repeated clashes with Chinese authorities caused Google to reconsider its decision on many occasions, the former executives said. Things almost collapsed in 2008, when Chinese government officials asked Google to censor results not only on Google.cn but also on Google.com. the company's English-language search engine. Google refused, and after the 2008 Olympics, Chinese officials dropped the issue.

Google now says it thinks that its attempt to help bring openness to China has failed.

"We were looking at an environment that is more difficult than it was when we started," Mr. Drummond said in an interview on Tuesday. "Far from our presence helping to open things up, it seems that things are getting tighter for open expression and freedom."

Robert Gibbs, the White House press secretary, said Wednesday that the White House had been briefed by Google on the company's decision. However, he declined to describe what actions the government might take in response to the claims of Chinese-directed Internet attacks.

"The recent cyberintrusion that Google attributes to China is troubling, and the federal government is looking into it," said a White House spokesman, Nicholas Shapiro. He said that the president had stated that Internet freedom was a central human rights issue on a recent China trip. He also said that the president had made Internet security a national priority.

Gabriel Stricker, a Google spokesman, said Google's decision to publicize the attacks was motivated in part by its desire to alert activists that their accounts could have been compromised.

A company finds a censorship battle is still going on.

The attacks present a challenge for the Obama administration, which last year debated the role of a federal Internet security adviser. The administration is grappling on how to balance stricter security controls and the freedom of technology companies to innovate.

Several Internet security specialists were quick to point out that a group within the White House led by Lawrence H. Summers, the national economic adviser, had pointed to Google in debates on the appointment as an example of an innovative Silicon Valley company that might be hamstrung by strict new Internet security restrictions.

"It's ironic that the new economy folks at the White House were pushing back against faster movement on cybersecurity to protect companies like Google from stricter regulations," said James Lewis, an Internet security specialist at the Center for Strategic and International Studies in Washington. Last year, Mr. Lewis led a bipartisan study calling for the creation of a strong Internet czar reporting directly to the president to combat a rash of new security threats.

The White House said on Tuesday that Robert A. Schmidt, a compromise candidate who was chosen last month to be the Internet security adviser, would not start in the position until later in the month.

GILLES SABRIE FOR THE NEW YORK TIMES

Google's office in Beijing. The company has warned some users their accounts were hacked.

Recent Network Attacks

A selection of suspected Chinese cyberattacks on American companies and agencies, as well as other foreign networks.

AUG. 2006
U.S. Department of Defense

Officials announce that Chinese hackers downloaded 10 to 20 terabytes of data from the military's unclassified network, NIPRNet.

NOV. 2006
U.S. Naval War College

The college's computer infrastructure is attacked by Chinese hackers, shutting down campus Web and e-mail systems for two weeks.

AUG. 2007
Britain, France, Germany

The British Security Service, the French prime minister's office and the office of the German chancellor complain to China about attacks on government networks.

OCT. 2007
Oak Ridge National Lab

Hackers send e-mail messages to more than 1,000 employees at this Department of Energy laboratory. The e-mail attachment, when opened, provides access to internal databases. China is suspected as the source.

OCT. 2008
Certain Skype users

Computer security researchers at the University of Toronto discover a Chinese surveillance system that records text chats between Chinese Skype users and users outside of China.

MARCH 2009
103 countries

University of Toronto researchers say that a vast electronic spying system primarily controlled from computers in China had infiltrated at least 1,295 computers in 103 countries.

DEC. 2009
Companies and individuals

China-based hackers attack at least 34 companies, including Google and Adobe. The Gmail accounts of human rights activists in the U.S., China and Europe are particular targets.

Sources: Center for Strategic and International Studies; Northrop Grumman

THE NEW YORK TIMES

The New York Times

NEW YORK, FRIDAY, JANUARY 15, 2010

U.S. Treads Lightly in Wake of Google's Loud Stance on China

By DAVID E. SANGER and JOHN MARKOFF

SANTA CLARA, Calif. — Last month, when Google engineers at their sprawling campus in Silicon Valley began to suspect that Chinese intruders were breaking into private Gmail accounts, the company began a secret counteroffensive.

It managed to gain access to a computer in Taiwan that it suspected of being the source of the attacks. Peering inside that machine, company engineers actually saw evidence of the aftermath of the attacks, not only at Google, but also at at least 33 other companies, including Adobe Systems, Northrop Grumman and Juniper Networks, according to a government consultant who has spoken with the investigators.

Seeing the breadth of the problem, they alerted American intelligence and law enforcement officials and worked with them to assemble powerful evidence that the masterminds of the attacks were not in Taiwan, but on the Chinese mainland.

But while much of the evidence, including the sophistication of the attacks, strongly suggested an operation run by Chinese government agencies, or at least approved by them, company engineers could not definitively prove their case. Today that uncertainty, along with concerns about confronting the Chinese without strong evidence, has frozen the Obama administration's response to the intrusion, one of the biggest cyberattacks of its kind, and to some extent the response of other targets, including some of the most prominent American companies.

President Obama, who has repeatedly warned of the country's vulnerability to devastating cyberattacks, has said nothing in public about one of the biggest examples since he took office. And the White House, while repeating Mr. Obama's calls for Internet freedom, has not publicly demanded a Chinese government investigation. Secretary of State

Continued on Page A10

From Page A1

Hillary Rodham Clinton, who had been the most senior U.S. official to talk of the seriousness of the breach, discussed it on Thursday with a Chinese diplomat in Washington, however, and a senior administration official said there would be a "démarche in coming days" — a diplomatic move.

On Thursday, China's Foreign Ministry deflected questions about Google's charges and dismissed its declaration that it would no longer "self-censor" searches conducted on google.cn, its Chinese search engine. A ministry spokeswoman said simply that online services in China must be conducted "in accordance with the law."

In interviews in which they disclosed new details of their efforts to solve the mystery, Google engineers said they doubted that a nongovernmental actor could pull off something this broad and well organized, but they conceded that even their counterintelligence operation, taking over the Taiwan server, could not provide the kind of airtight evidence needed to prove the case.

The murkiness of the attacks is no surprise. For years the National Security Agency and other arms of the United States government have struggled with the question of "attribution" of an attack; what makes cyberwar so unlike conventional war is that it is often impossible, even in retrospect, to find where the attack began, or who was responsible.

The questions surrounding the Google attacks have companies doing business in China scrambling to confirm that they were victims. Symantec, Adobe and Juniper Networks acknowledged in interviews that they were investigating whether they had been attacked. Northrop and Yahoo, also described as subjects of the attacks, declined to comment.

Besides being unable to firmly establish the source of the attacks, Google investigators have been unable to determine the goal: to gain commercial advantage; insert spyware; break into the Gmail accounts of Chinese dissidents and American experts on China who frequently exchange e-mail messages with administration officials; or all three. In fact, at least one prominent Washington research organization with close ties to administration officials was among those hacked, according to one person familiar with the episode.

Even as the United States and companies doing business in China assess the impact, the attacks signal the arrival of a new kind of conflict between the world's No. 1 economic superpower and the country that, by year's end, will overtake Japan to become No. 2.

It makes the tensions of the past, over China's territorial claims or even the collision of an American spy plane and Chinese fighter pilots nine years ago, seem as outdated as a grainy film clip of Mao reviewing the May Day parade. But it also lays bare the degree to which China and the United States are engaged in daily cyberbattles, a covert war of offense and defense on which America is already spending billions of dollars a year.

Computer experts who track the thousands of daily attacks on corporate and government computer sites report that the majority of sophisticated attacks seem to emanate from China. What they cannot say is whether the hackers are operating on behalf of the Chinese state or in a haven that the Chinese have encouraged.

The latest episode illuminates the ambiguities.

For example, the servers that carried out many of the attacks were based in Taiwan, though a Google executive said "it only took a few seconds to determine that the real origin was on the mainland." And at Google's headquarters in Mountain View, there is little doubt that Beijing was behind the attacks. Partly that is because while Mr. Obama was hailing a new era of cautious cooperation with China, Google was complaining of mounting confrontation, chiefly over Chinese pressure on it to make sure Chinese users could not directly link to the American-based "google .com" site, to evade much of the censorship the company had reluctantly imposed on its main Chinese portal, google.cn.

Reluctant to accuse a suspect when guilt can't be proved.

"Everything we are learning is that in this case the Chinese government got caught with its hand in the cookie jar," said James A. Lewis, a senior fellow at the Center for Strategic and International Studies in Washington, who consulted for the White House on cybersecurity last spring. "Would it hold up in court? No. But China is the only government in the world obsessed about Tibet, and that issue goes right to the heart of their vision of political survival and putting down the separatists' movements."

Over the years, there have been private warnings issued to China, notably after an attack on the computer systems used by the office of the defense secretary two years ago. A senior military official said in December that that attack "raised a lot of alarm bells," but the attacker could not be pinpointed. The administration cautioned Chinese officials that attacks seemingly aimed at the national security leadership would not be tolerated, according to one American who took part in delivering that message.

David E. Sanger reported from Santa Clara, and John Markoff from San Francisco. Mark Landler contributed reporting from Washington.

Business Day

The New York Times

SATURDAY, JANUARY 16, 2010

Scaling the Digital Wall in China

A Few Internet Users Find Ways Around Government Filters

By BRAD STONE and DAVID BARBOZA

The Great Firewall of China is hardly impregnable.

Just as Mongol invaders could not be stopped by the Great Wall, Chinese citizens have found ways to circumvent the sophisticated Internet censorship systems designed to restrict them.

They are using a variety of tools to evade government filters and to reach the wide-open Web that the Chinese government deems dangerous — sites like YouTube, Facebook and, if Google makes good on its threat to withdraw from China, Google.cn.

It's difficult to say precisely how many people in China engage in acts of digital disobedience. But college students in China and activists around the world say the number has been growing ever since the government stepped up efforts to "cleanse" the Web during the Beijing Olympics and the Communist regime's 60th anniversary last year.

As part of that purge, the Chinese government shut down access to pornography sites, blogs, online video sites, Facebook, Twitter and more.

While only a small percentage of Chinese use these tools to sidestep government filters, the ease with which they can do it illustrates the difficulty any government faces in enforcing the type of strict censorship that was possible only a few years ago.

Jason Ng, a Chinese engineering school graduate who will say only that he works in the media business, wakes every day at 8:30 a.m., and then begins his virtual travels through an open, global network by *fanqiang*, or "scaling the wall." He connects to an overseas computer with a link, called a proxy server, that he set up himself. It costs 15 renminbi, or around $2, a month to share with about two dozen other friends.

Mr. Ng then works on his blog and checks the news on Google Reader and Twitter to "officially start my day of information." Chinese citizens engaged in such practices say the government rarely cracks down on them individually, preferring instead to go after prominent dissidents who publish information about forbidden topics online.

As a result, college students, human rights

Continued on Page 4

From First Business Page

activists, bloggers, journalists and even multinational corporations in China are rushing to use tools that go over or around barriers set up by Chinese regulators, in part because they feel it is the only way to participate in a global online community.

Isaac Mao, a well-known blogger and activist in China, says the number of people seeking access to blocked sites has grown as more and more popular Web sites have been shut down by Beijing.

These digital dissidents have begun to organize small conferences and networks to share information and tricks about how to get access to banned material. "People start to hold a grudge against the government for depriving them of access to the Web sites they regularly visit," Mr. Mao says.

But as the government has expanded its control over Internet, it has also intensified efforts to close some of the channels being used to evade the online blockade. The result has been a technological game of cat and mouse between the Chinese government and a global contingent fighting for online freedoms.

AnchorFree, a start-up based in Sunnyvale, Calif., has built a profitable business by providing free, advertising-supported software called Hotspot Shield that tunnels about 7.5 million people around the world into the Internet by encrypting Internet users' data and cloaking their identities.

But last summer, the Chinese government blocked AnchorFree's Web site so that Chinese citizens could no longer download the software. Almost immediately, its users began e-mailing their own copies of the program to friends and posting links to other sites that hosted it. The program's use in China has doubled since then, said David Gorodyansky, AnchorFree's founder.

Beijing parries a global contingent for online freedoms.

Other censorship-evading tools have been created by nonprofit companies trying to combat authoritarian governments and by former Chinese citizens who, in many cases, want to help fellow members of persecuted minority groups still in the country.

Several such tools were created by a group called G.I.F., or Global Internet Freedom. It was founded in 1999 by members of the Falun Gong sect living in the United States as a way to get unfettered information about their practice into the country by e-mail. About a million people in China now use the service, which is maintained by about 50 volunteers around the world.

Users must download the G.I.F. programs and then every time they use servers, find the Internet Protocol addresses, or online coordinates, of servers around the world. G.I.F. volunteers try to distribute these coordinates through a multitude of channels, like instant-messaging services.

David Tian, a NASA engineer in Maryland who says he works harder at night on G.I.F. than he does during the day on weather satellites, says that officials from the Chinese government have begun posing as G.I.F. users, so they can intercept those I.P. addresses and block them. In turn, G.I.F. volunteers now work to identify these government officials and track them, so they can keep the information out of their hands.

An even bigger challenge, Mr. Tian said, is keeping up with the rapidly growing demand for the service from countries like China and Iran. "The bottleneck is not their firewall, it's our capacity," he said. "We have to limit bandwidth to what we can afford, so when there are a lot of users, some have to wait."

Many of these organizations are hoping the United States government will help out with money. Since the 2008 budget year, Congress has appropriated nearly $50 million for tools that encourage "Internet freedom," though only a small portion of that money has yet been handed out.

One problem, says Michael J. Horowitz, a fellow at the Hudson Institute, a conservative policy research group, is that that the federal government appears reluctant to pay for efforts associated with groups that alienate the Chinese government.

"Many of these guys are Falun Gong practitioners and the State Department doesn't want to aggravate China," he said. "China goes more nuclear at the mention of Falun Gong than any other two words in the whole dictionary."

Despite these bureaucratic battles, people on the side of greater Internet freedoms in the continuing fight against Big Brother say the battlefield is inherently tilted in their favor.

"The architecture of the Internet makes our work easier," said Bill Xia, a programmer based in North Carolina whose software tools, including DynaWeb and FreeGate, are used by hundreds of thousands of people in China every day to access forbidden sites. "The starting point of the Internet is open networks. Everybody can publish and receive data, and unless they want to shut down the whole Internet, we have the advantage."

Brad Stone reported from San Francisco and David Barboza from Shanghai. Dan Levin contributed reporting from Beijing, and Bao Beibei contributed research from Shanghai.

PHILIPPE LOPEZ/AGENCE FRANCE-PRESSE -- GETTY IMAGES

A cafe in Shanghai. Some say the government mostly trains its efforts on prominent dissidents who publish information about forbidden topics online.