2011 Circumvention Tool Evaluation

Hal Roberts, Ethan Zuckerman, and John Palfrey

Berkman Center for
Internet & Society

August 2011

Each co-author is affiliated with The Berkman Center for Internet & Society at Harvard University. Hal Roberts is a fellow; Ethan Zuckerman is a senior researcher; and John Palfrey is a faculty co-director of the Berkman Center. We gratefully acknowledge support for this research from the US Department of State via a subgrant through Internews Network (USA).

PREFACE

The importance of the Internet as a digital public sphere (Benkler) has become increasingly apparent with the dramatic events of the Arab Spring, a series of uprisings throughout North Africa and the Middle East that have unseated leaders and transformed societies. While political scientists will spend the next decade arguing over whether the Internet was one of the primary factors in the spread of the protests or simply a contributing factor, early evidence suggests that activists used the Internet both to plan and to disseminate information about protests.

The shutdown of the Internet by the governments of Egypt and Libya, and the slowdown of net connectivity in Bahrain suggests that governments are increasingly willing to take dramatic measures to control online speech. While the OpenNet Initiative, a research consortium led by John Palfrey and Jonathan Zittrain at the Berkman Center, Ron Deibert at the University of Toronto and Rafal Rohozinski of the SecDev Group, has been documenting state censorship of the Internet since 2002, reports of complete Internet shutdown had been rare. Myanmar shut down connectivity completely in the wake of the 2007 Saffron Revolution protests, and China disconnected the restive province of Xinjiang from the Internet for 10 months in 2009-2010 in the wake of riots in Urumqi. The Egyptian Internet shutdown affected many more Internet users than any earlier events and suggests that governments may be willing to suffer the economic and public relations damage that results from such a shutdown in an attempt to keep popular uprisings in check.

The dictator's dilemma (proposed by former US Secretary of State George Shultz in 1985) suggests that totalitarian leaders have a choice between permitting new communication technologies and accepting their potential to be used to subvert their rule, or blocking access to those tools and suffering slower economic growth. Recent events in the Arab world suggest we're seeing the emergence of a related "digital dilemma".[1]

Faced with widespread public protests, on January 13, Tunisian president Zine El Abidine Ben Ali made a series of promises to his people: a reduction in prices of staple foods, instructions to the military not to shoot protesters, and a promise to end Internet filtering. While Facebook was a powerful tool for protesters who opposed his rule, Ben Ali realized that ending an unpopular policy of Internet filtering was a concession he could offer to Tunisia's 3.6 million Internet users (34% of the population.) Faced with similar circumstances on January 27th, Hosni Mubarak elected to shut down Egypt's Internet, which previously had been largely unfiltered. While both leaders ultimately ceded their posts, their different reactions to the digital dilemma suggest that authoritarian rules are still trying to determine how to navigate these waters.

Given the rising awareness of the potential of the Internet as a political space and increasing government control over the space, it is easy to understand the widespread interest in finding technical

[1] "Communication and Democracy: Coincident Revolutions and the Emergent Dictators," 1997, http://www.rand.org/pubs/rgs_dissertations/RGSD127.html.

solutions to Internet filtering. While filtering circumvention technologies emerged in 1996 with Bennet Hazelton's Peacefire, designed to evade filtering within US high schools and universities, in recent years, there's been a great deal of interest in the technical community and the general public in the topic of Internet circumvention. The embrace of an "Internet freedom" agenda by US Secretary of State Hillary Clinton in a pair of widely publicized speeches has increased awareness of the challenges of Internet filtering and encouraged new actors to explore or enter the field.

The prospect of expanded fiscal support for tool development and deployment has led to debate in the popular press about the strengths and weaknesses of various circumvention tools and strategies. These debates make clear the need for scholarly research on the efficacy of various tools.

In 2007, the Berkman Center conducted an in-depth evaluation of nine prominent filtering circumvention tools. We released our findings and methodology in 2009 both to help inform debate and to provide possible research frameworks for other researchers. The 2007 study was wide in scope—we considered six factors in our analysis: utility, usability, security, promotion and marketing, fiscal sustainability, and openness. It was also very difficult to conduct, as it centered on in-country testing, which required a researcher to travel to China, Korea and Vietnam to conduct tests.

Subsequent to that report, we've seen other evaluation efforts focus on the usability of circumvention tools (Freedom House's "Leaping Over the Firewall" report)[2], the security of circumvention tools ("Ten Things to look for in a Circumvention Tool" from Roger Dingledine of Tor)[3], or instructions for using the tools ("How to Bypass Internet Censorship Manual")[4]. While useful, these evaluations do not include detailed, documented performance testing of these tools either in the lab or in filtered countries, which means they are not able to report on whether tools work in a particular censored environment and whether they load webpages accurately and quickly (Freedom House's report provides a top level performance metric but no indication for the method used to generate that score).

This study uses a novel methodology for conducting in-country testing without requiring a researcher to be physically present in censored nations. While this method does not fully replicate the performance of circumvention tools from a cybercafé in a filtered nation, it can be regularly replicated, allowing us to conduct tests over a long period of time and, potentially, create an ongoing, regularly updated portrait of circumvention tool usability in locations across the globe. In this report, we focus on questions of utility—the ability for a tool to be installed and used in a particular location, and the accuracy and speed of the tool. Additionally, we address concerns about security, usability and openness when appropriate.

This evaluation also differs from our 2007/2009 work in that we cover significantly more tools and examine two classes of tools (ad-supported proxy servers and VPN services) which we did not review previously. We expanded the set of tools considered to recognize the increased number of options that

[2] Cormac Callanan, Hein Dries-Ziekenheiner, Alberto Escudero-Pascual, and Robert Guerra, Leaping Over the Firewall: A Review of Censorship Circumvention Tools. Freedom House, 2011, http://www.freedomhouse.org/template.cfm?page=383&report=97.

[3] R. Dingledine, Ten Things to Look for in a Circumvention Tool. The Tor Project, 2010, https://www.torproject.org/press/presskit/2010-09-16-circumvention-features.pdf.

[4] "How to Bypass Internet Censorship Manual," https://howtobypassInternetcensorship.org.

users in censored nations may choose from, and to acknowledge results of our previous research which suggest that simple web proxies and VPNs have a very significant user base in comparison with dedicated censorship circumvention tools.

We strongly encourage readers of this report to consider our findings here in context of our other recent research. Our 2010 Circumvention Tool Usage Report finds that usage of all circumvention tools is quite small in comparison to the overall number of Internet users in nations that experience acute Internet filtering.[5] In that report, we project that fewer than 3% of Internet users in nations that filter the Internet aggressively use VPNs, ad-supported proxies or dedicated circumvention tools to circumvent Internet censorship.

Our 2010 Report on Distributed Denial of Service (DDoS) Attacks suggests that it is a mistake to consider Internet filtering to be the sole barrier to unfettered access to the Internet as a digital public sphere.[6] We report on the rise of DDoS, site hijacking and other attacks designed to silence the publishers of controversial speech, not simply to prevent audiences from accessing their sites. We believe these sorts of attacks are on the rise—as we draft this report, leading Malaysian political website, Malaysiakini, is under sustained DDoS attack, preventing it from reporting in the run-up to elections in Sarawak state.[7] As important as circumvention tools are in enabling unfettered Internet access, they offer no protection against attacks that directly affect publishers either by taking their sites offline or intimidating or arresting authors into silence.

SUMMARY OF FINDINGS

- We identified 19 tools to test and tested 17, including five tools which we had tested in 2007. The set of tools we tested includes all circumvention tools mentioned by name by a set of political and independent media bloggers contacted in a survey conducted in 2010 by the Berkman Center, along with the three VPN services and five simple web proxies with the largest user base (as determined by a survey conducted as part of our 2010 Circumvention Usage study.) In addition to the tools mentioned by name in the survey, we included three tools which use interesting or unconventional circumvention strategies.

- We evaluated the tools in terms of utility (were they able to connect to blocked webpages?), accuracy (did they correctly download webpages?) and speed by using testing servers in China,

[5] H. Roberts, E. Zuckerman, J. York, R. Faris, and J. Palfrey, "2010 Circumvention Tool Usage Report, Berkman Center for Internet & Society, 2010, http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage.

[6] E. Zuckerman, H. Roberts, R. McGrady, J. York, and J. Palfrey, "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites," Berkman Center for Internet & Society, 2010, http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights.

[7] A. Lian, "Malaysiakini under DDOS attack ahead of Sarawak election tomorrow," Temasek Review Emeritus, April 15, 2010, http://www.temasekreview.com/2011/04/15/malaysiakini-under-ddos-attack-ahead-of-sarawak-election-tomorrow/.

South Korea, Vietnam and the United Arab Emirates, as well as setting test baselines from our servers in the United States. In each test country, we rented a Virtual Private Server, installed Windows Server 2003 and installed/accessed each of the 19 tools.

- In each country, we tested the performance of the tool on a set of 40 sites. The test sites were different for each country—we selected the 20 sites that Google Ad Planner listed as most popular in the country, and a subset of 20 sites which OpenNet Initiative reported as being blocked within the country. The popular sites test the usability of the tool for use in routine browsing, while the blocked sites test the utility of the tool in circumventing censorship. We ran tests on two separate occasions, in February 2011 and in March 2011. For each requested page, we logged the time elapsed for downloading the page, ran a basic test to verify that the page had returned correctly, and stored a screenshot of the resulting page in the browser.

- In contrast to our research in 2007, which found that virtually all tools tested were able to access blocked sites, our current research finds several tools which were not usable in one or more of our test beds. Our results differ between nations, which suggests some tools are blocked in some countries and not in others, and differences in behavior between February and March tests suggest that filtering and blocking policies employed by states change over time.

- Our analysis of error rates suggests that the task of delivering rich content through a proxy is a difficult task and that not all tools are able to consistently deliver content in an error-free fashion.

- One of the major conclusions of our 2007 report was that tools worked but were significantly slower than accessing the Internet directly (i.e., not through a circumvention tool.) That finding holds true in 2011 as well, though load time varies greatly both between tools and within tests of the same tool. It is not possible to compare tool speed in this test directly with previous results, as the sites tested and the testing setup differ substantially from the 2007 tests.

- We believe that developers of circumvention tools are currently challenged to solve three difficult problems: keep tools useable in the face of government efforts to block them; accurately render complex, rich content; and deliver content quickly. Tools that attempt to provide additional functionality, like providing a high degree of user anonymity, face additional challenges.

  In our previous analysis, we saw little evidence that the tools we studied were being blocked by governments. We now see extensive evidence of government blocking, and it is clear that several tool developers are engaged in sophisticated cat-and-mouse games with government adversaries. This circumstance is confirmed by recent media reports about increased Chinese blocking of circumvention tools.[8] We also saw fewer errors in rendering content in 2007 than in the current analysis—in this case, the increase is not likely due to increased filtering, but due to the rising complexity of popular webpages. These factors combine to make the tasks facing developers of circumvention tools more challenging and daunting, and suggest that, in some cases, governments may be proving more effective at blocking tools than software providers are at evading their controls.

BACKGROUND

What follows below is a very brief overview of the techniques of Internet filtering and responses used by circumvention tool developers. Users seeking more background are encouraged to refer to our 2007 report, which includes extensive explanations on this topic.

The OpenNet Initiative has documented network filtering of the Internet by national governments in over forty countries worldwide.[9] Countries use this network filtering as one of many methods to control the flow of online content that is objectionable to the filtering governments for social, political, and security reasons. Filtering is particularly appealing to governments as it allows them to control content not published within their national borders. In addition to national Internet filtering by governments, many schools and businesses filter their local connections to the Internet. And many web sites even filter their own content by the geographic location their users—for example, the television streaming site hulu.com blocks all users outside of the U.S. from accessing its content.

All circumvention tools use the same basic method to bypass this sort of network filtering: they proxy connections through third party sites that are not filtered themselves. By using this method, a user in China who cannot reach http://falundafa.org directly can instead access a proxy machine like http://superproxy.com/, which can fetch http://falundafa.org for the user. The network filter only sees a connection to the proxy machine (superproxy.com), and so as long as the proxy itself remains unfiltered, the user can visit sites through the proxy that are otherwise blocked by the network filter. Some, but not all, tools also encrypt traffic between the user and proxy, both so that the traffic between the user and proxy is more resistant to surveillance and to defeat filtering triggered by the content of the traffic, rather than by the destination of the traffic.

Despite this core similarity, circumvention tools differ significantly in many implementation details. For the purpose of this report, we break circumvention tools into four large categories based on their proxy implementations. Each category of tool is distinguished from one another also by virtue of each being closely associated with a single model of financial support. The four categories of tools are simple web proxies, virtual private network (VPN) services, HTTP/SOCKS proxies, and "custom" tools.

[8] S. Lafraniere and D. Barboza, "China Tightens Electronic Censorship," The New York Times, March 21, 2011, https://www.nytimes.com/2011/03/22/world/asia/22china.html.

[9] R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, 1st ed. The MIT Press, 2010, http://www.access-controlled.net/.

Simple web proxies are server-side applications accessed through web page forms. To use one of these tools, the user simply visits a web page that includes a url input box. Instead of entering a web page url into the browser address bar, the user enters the address into the web page form. By submitting this web page form, the user sends the url request to the proxy web server, and the web server returns the page via the proxy. Simple web proxies do not require the user to download or install any client-side application. To use the tool the user needs only visit the web page hosting the proxying web application (for instance http://superproxy.com). But simple web proxies do require that users navigate the separate, form-based browsing interface, rather than using the address box on their web browser to enter destination site names.

Almost all simple web proxies support themselves by hosting ads. Ads are generally hosted on an initial landing page and are often inserted into proxied web pages. Some tools go a step further and attempt to replace ads on the requested page with their own ads. Simple web proxies were initially targeted at students in the U.S. and other countries to bypass school filtering systems, but they use the same basic proxying methods as the blocking-resistant tools and therefore also serve to bypass national filters as long as a given proxy is not specifically blocked by a given country.

Some simple proxies have been optimized for usage in countries where the Internet is filtered by the government. At least one very widely used proxy site markets itself to users from a specific country who seek access to YouTube, which is blocked by their government. For the most part, these tools have only the weakest defenses against government blocking—some attempt to disguise their function on the front pages in hopes of evading blocking, while some change IP addresses in hopes of evading IP blocking. Some simple proxies register closely related domain names in anticipation of being blocked, and many of their users know that if 1superproxy.com ceases working in their country, they might try 2superproxy.com.

Virtual Private Network (VPN) Services use software that implements a networking protocol to encrypt and tunnel all Internet traffic through a proxy machine. VPN technology has traditionally been used to allow corporate and other institutional users to access internal networks from the public Internet, but in the past few years there has been tremendous growth in the availability of personal VPN services. Among other uses, these personal VPN services act as circumvention tools as long as the VPN proxy is hosted outside a filtering country. VPN services might or might not require installation of client-side software and allow the user to access the web directly through the native browser interface (many rely on existing VPN support in Windows or Mac OSX and so need no extra client software). Because VPN services tunnel all Internet traffic, they can be used for email, chat, and any other Internet service in addition to web browsing.

Almost all VPN tools support themselves through fees charged directly to users (charges of $10 to $30 per month are common), though a few also offer free services with restricted bandwidth. The exception to this business model is Hotspot Shield, overwhelmingly the most popular VPN service, which charges no fees but supports itself by injecting ads into the top of all web pages served through its service.

HTTP/SOCKS proxies are application level proxies that funnel network traffic through protocols designed to allow web traffic to pass through firewalls. Users generally find lists of these proxies in the form of IP addresses and port numbers on proxy directory web sites. To use a given HTTP or SOCKS proxy, the user enters the IP address and port number of the proxy into a configuration screen of the browser. As a result, no client-side application is needed. The user is able to use the native interface of the browser. These proxies are generally open to the public and have no readily identifiable source of funding (users do not pay to subscribe to them, and the owners of the proxies are anonymous so there is no way to know if they are receiving charitable or government funding). These tools have no blocking resistance and can be challenging for novice users to use. While it is impossible to accurately estimate how widely these tools are used, we believe they are used less often than web proxies. No HTTP/SOCKS proxies were tested in this study.

The rest of the tools tested, which we put in the **custom tools** category, are not as easily categorized. All of the remaining tools use the same basic technology of proxying connections through an unfiltered computer to bypass filtering, but they have widely differing implementations of that basic method of proxying. All of the tools in this category require execution of a downloaded, client-side application but use the native interface of the browser for web access, like HTTP/SOCKS proxies and unlike simple web proxies. Many, but not all, of these tools include some level of blocking resistance. In many cases, robust blocking resistance is one of the key features of the tool (in our 2010 Circumvention Tool Usage Report, we called these tools "blocking resistant tools," but we change the label to "custom tools" in this report to include tools that are not VPNs, simple web proxies, or HTTP/SOCKS proxies but also do not have significant blocking resistance features).

Blocking Resistance is becoming a major challenge for circumvention software developers. Governments that block access to sensitive websites usually also block access to circumvention tools. China can block superproxy.com as easily as they can block falundafa.org. Even for tools that are not simple web proxies, blocking access to the proxies used by the tool (whether the proxies are VPNs, HTTP/SOCKS proxies, or some other form of proxy) will prevent the tool from working. Some countries also block tools either by blocking the protocol used by the tool (for instance blocking a specific VPN protocol) or by blocking all traffic matching some traffic signature that defines a tool (for instance, blocking traffic to a specific TCP port used by a circumvention tool).

Simple forms of blocking resistance include registering many IP addresses that are served by a single domain name or registering many domain names, so that a user can use an alternative domain once the main name is blocked. Some of the tools we consider in this report use much more sophisticated forms of blocking resistance, including automatically switching between a large pool of constantly changing proxies and obfuscating proxy traffic to defend against traffic signature blocking. We discuss the blocking resistance features of specific tools in more detail below.

Trust and security should be a major consideration for circumvention tool users, though it too seldom is for tool developers. With one notable exception, proxy systems give their operators a great deal of power to examine the traffic passing through their systems. While an Internet service provider in China cannot determine that a specific encrypted proxy user is accessing falundafa.org, the proxy owner can.

Operators of simple web proxies take advantage of this fact to make their ad inventory more appealing to clients—if a proxy is widely used to access gambling sites, it may be an attractive locale for online poker advertisements. Other proxy servers have, in the past, offered to sell aggregated user data to advertisers and online marketers, a major invasion of privacy and a potentially serious security risk.

It has been speculated, though not proven, that some governments that filter the Internet might run "honeypot" proxies, designed to monitor user behavior and discover what sites proxy users are visiting, presumably to add sites to their lists of blocked sites and, more troublingly, to snoop the personal information of activists and their social networks. Running such a honeypot proxy would be trivially easy for even the smallest, least technically sophisticated national government.

The Tor system is architected to sharply reduce the trust users need put in proxy operators. Rather than using a single proxy, which can be easily monitored, the Tor network consists of thousands of proxies, operated by different volunteer operators. A request for a webpage is routed through three of these proxies, selected at random. Each proxy knows about only part of the routing chain—while the "exit node" proxy can monitor what sites are being visited, it cannot connect that information to the Internet address of the user utilizing the system. As a result, it is extremely difficult to monitor the behavior of an individual user through Tor, something that is easily and routinely accomplished with other proxy services. However, Tor's architecture is significantly more complex than that of other proxies, which means the system is often slower than some of the other tools. For users deeply concerned about online security, this is likely a worthwhile tradeoff: reduced speed for enhanced privacy.

TOOL EVALUATIONS

We planned to test 19 tools. Eight were tools explicitly named by bloggers affiliated with Global Voices as tools they used to circumvent Internet censorship. Five were the most popular simple web proxies as determined by our work for our Circumvention Usage report. Three were the most popular VPNs, again according to our work for our Circumvention Usage report. Three were tools we find particularly interesting, because they use unusual methods to circumvent censorship.

Two of the popular simple web proxies no longer exist. Web proxies go out of business frequently so it is possible that the operators of these proxies decided they were not able to turn a profit with these sites (though very popular web proxies do not often go out of business). We worry, however, that a recent Chinese crackdown on proxies may have forced these sites to go out of business, either by blocking them so aggressively that they were no longer useful, or by contacting the proxy owners. Both of these web proxies had China-focused interfaces but had been operating uninterrupted for at least two years.

For each tool, we tested the latest, version available from the tool's web site, with preference for free over pay versions. Many projects offer multiple different tools (some even offer a full range of choices between HTTP, SOCKS, simple web, and VPN proxies), and it was beyond the resources of this study to test many versions of each tool. We tried to test the version of each tool that we thought will be most widely used, which means testing the simplest version of proxy and, where available, selecting the free version of each tool. Some tools also offer newer versions of their tools through informal channels. We still used the version of the tool provided on the tool's web site in each of these cases, again because we thought the version provided on the web site was likely to be the most widely used.

For this public report, we provide only anonymized results for specific tools, for fear of providing a roadmap that filtering countries could use to shut down the evaluated tools.

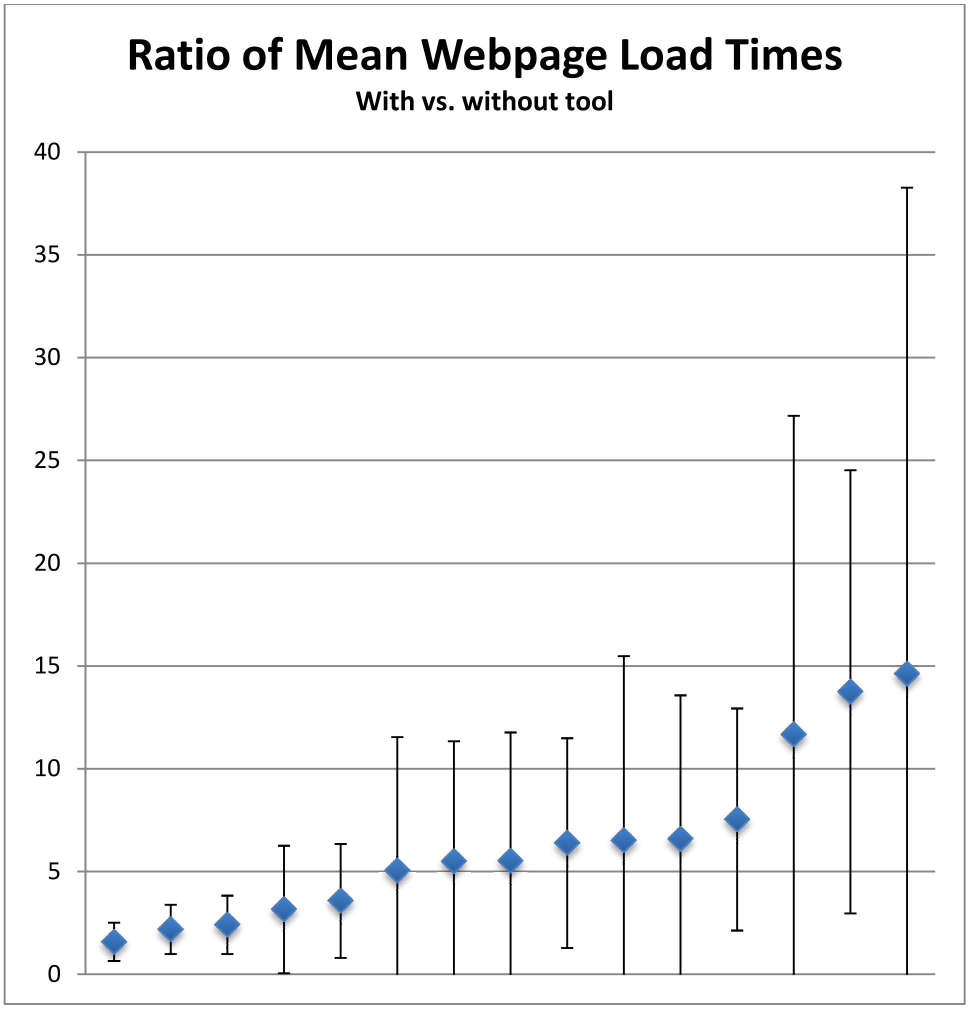
RESULTS

Tool	**China: February**	**China: March**	**Korea: February**	**Korea: March**	**UAE: February**	**UAE: March**	**Vietnam: February**	**Vietnam: March**
Simple Web Proxies								
A	pass	pass	pass	Pass	blocked	blocked	pass	pass
B	blocked	blocked	broken	broken	blocked	blocked	broken	broken
C	pass	pass	pass	Pass	blocked	pass	pass	pass
D	pass	pass	pass	Pass	pass	pass	pass	pass
VPNs								
E	blocked	blocked	pass	bad test	install failed	install failed	pass	bad test
F	pass	pass	bad test	bad test	bad test	bad test	bad test	bad test
G	bad test	pass	bad test	bad test	bad test	bad test	bad test	bad test
H	pass	pass	pass	pass	install failed	bad test	pass	pass
Ot tools								
I	pass	pass	pass	timed out	timed out	pass	pass	timed out
J	install failed	install failed	pass	bad test	install failed	install failed	install failed	install failed
K	Pass	blocked	pass	pass	blocked	blocked	pass	pass
L	pass	pass	blocked by tool	blocked by tool	blocked by tool	blocked by tool	blocked by tool	blocked by tool
M	blocked	blocked	bad test	pass	pass	blocked	pass	blocked
N	blocked	pass	pass	pass	pass	pass	pass	pass
O	pass	partial block	pass	pass	pass	pass	pass	pass
P	pass	pass	pass	pass	pass	pass	pass	pass
Q	blocked	blocked	broken	broken	blocked	broken	broken	broken

Key	
Pass	Tool performed as expected
bad test	Tool unblocked, but could not be tested
partial block	Some sites were accessible, others blocked, pattern unclear
broken	Tool unblocked, but pages were not readable when delivered
install failed	Tool could not be installed, access to key component blocked
blocked	Tool installable, but blocked and unusable in country
blocked by tool	Tool does not permit use in country
timed out	Tool installable, not obviously blocked, but does not retrieve pages

For all tools, the most important question is whether the tool can be used in the censored country. As displayed above, the utility of tools varies widely. Only two of the seventeen tested tools were usable in all countries where we tested them, during both tests. (It is possible, and perhaps likely, that two VPN tools were also usable in all countries, though our tests were not able to verify their utility.) Other tools were blocked in key countries, uninstallable, or produced webpages that were broken to the point of unreadability.

It is worth noting that China and UAE appear to have taken more aggressive steps than Vietnam and South Korea to block access to circumvention systems. Six systems failed both tests in China, and four in UAE. One tool failed both tests in Vietnam and none of the tools failed both tests in South Korea.



We also evaluate the time it takes to load different web pages using each tool compared to not using the tool from the same connection. These tests—with and without each tool—were run from within each of the countries and the results averaged over all the countries. The chart above shows the ratio of load times for each tool to load each of the 20 unfiltered sites for each country compared to the same connection not using the tool. For example, a value of 6 on the y-axis means that it took on average 6 times as long to load the set of unfiltered sites through the given tool compared to not using the tool from the same connection. Mean web page load times are calculated from all pages a tool was able to load successfully. Some tools only proxy some web pages and so generated very fast performance data. Pages that took more than 3 minutes to load were removed from the set for the purpose of calculating means, as were the two pages that took longest to load for each tool.

Times to load web pages varied greatly—this is understandable, as some web pages contain more content and are more difficult to render than others. But this high variance means that the mean load time is not an especially helpful statistic without considering standard deviation. The error bars on the graph above show standard deviation—in many cases, the standard deviation is so high, a low bound is not shown on the chart.

It is worth noting that two of the tools that have the slowest load insert ads into web pages the user is viewing. It is possible that the speed of these tools in affected by calls to an external ad server, which can be time consuming. Two of the tools that scored best are subscription-supported VPNs. With subscription support, these tools are likely more lightly used than free tools, and the subscription fees can be used to support bandwidth and server costs. Some free tools, however, feature comparatively low page load times.

Tool	Errors	Pages Loaded	Error ratio
A	1	88	1.1%
B	2	133	1.5%
C	4	193	2.1%
D	10	307	3.3%
E	3	75	4.0%
F	4	98	4.1%
G	13	229	5.7%
H	8	113	7.1%
G	23	288	8.0%
H	6	74	8.1%
I	21	229	9.2%
J	38	307	12.4%
K	69	307	22.5%
L	87	268	32.5%

Tools varied widely in terms of their ability to correctly render webpages. We calculated errors by specifying a specific text string on target pages and checking to see whether the tool accurately loaded the string. In cases where we detected that the string had not loaded, we manually reviewed screen shots of the page as rendered by the browser during the test to confirm that errors had occurred.

Simple web proxies fared particularly badly on this metric. In both cases, errors came from the challenge of parsing HTML, replacing references to urls in images, links, style sheets, and other html elements, and then reassembling the HTML for the user's browser. Simple web proxies particularly struggled with encoding issues for non-Latin character sets (including Chinese, Korean, and Arabic), causing the non-

Latin text to render as garbage on many web pages. VPNs fared reasonably well, as we might expect, as they are not attempting to interpret HTML.

For two other tools, we found evidence that outgoing requests from the tools' proxies were being blocked from accessing sites hosted *within* the filtering country, preventing the particular tool from accessing popular (unblocked) local sites and inflating the error rates for those tools. This behavior does not prevent users of those tools from accessing the local sites (which can be viewed simply by turning off the circumvention tool as needed), but it does make use of the tools less convenient.

DISCUSSION

When we presented our 2007 research, we were able to offer readers the reassurance that, while some tools were hard to use or had security flaws, those intended for use in circumventing censorship were able to do what they promised—allow users to access sites that were otherwise blocked in filtering countries. Four years later, the picture is not as encouraging. In China, a country targeted by many circumvention tool designers, six of the seventeen tools we tested failed entirely. If we add the two China-focused proxy sites we had hoped to test, that is eight of nineteen tested tools that do not work in China. We experienced a high rate of failure in UAE as well, suggesting that China's legendary "Great Firewall" is not the only difficult venue for circumvention tool designers.

For the past few years, blocking resistance has moved from a theoretical topic of discussion for tool developers to a major practical concern. Discussions with developers of tools that consistently avoid blocking suggests that blocking resistance is a primary concern in their tool architecture. A few tools have invested in developing their blocking resistance capabilities, and the blocking resistance features of those tools are more sophisticated than anything we saw developers proposing a few years back. The larger majority of tools, however, have few or no blocking resistance features, relying instead on the obscurity of relatively small user bases. According to the testing in this report, however, obscurity is an increasingly poor blocking resistance strategy, and even tools that invest in blocking resistance have to build increasingly sophisticated systems to remain functional.

The good news is that a core set of tool developers appear to be building solutions that continue to stay a step ahead of censors. The bad news is that censors appear to be using very aggressive methods to detect and block tools. For example, WiTopia has recently gone public with reports that many users in China are having difficulty accessing the service due to "China shenanigans." [10] Although we were unable to detect this blocking in our tests, others have reported that those shenanigans may have included blocking the popular VPN protocols PPTP and L2TP. [11] If this is the case, this would suggest a new approach to the dictator's dilemma in China, as VPNs are widely used by Chinese employees of foreign

[10] C. Young-Sam, "China 'Shenanigans' Hindering Web Users From Evading Censors, Witopia Says," Bloomberg News, 10-Mar-2011. http://www.bloomberg.com/news/2011-03-11/china-shenanigans-hinder-censor-evading-users-witopia-says.html

[11] O. Lam, "China: PPTP and L2TP VPN protocols blocked," Global Voices Advocacy, 11-Mar-2011. http://advocacy.globalvoicesonline.org/2011/03/20/china-pptp-and-l2tp-vpn-protocols-blocked/

companies to access business servers. Blocking the VPN protocol, rather than individual services, could have a serious adverse economic impact on the country.

We also see increasing evidence in our own tests, in media reports, and in discussions with circumvention tool developers that Chinese censors are increasing their use of traffic signatures to block circumvention tools. If authorities are beginning to block based on traffic signatures, a wide range of tools (those that use HTTPS proxies) may be at greater risk of blockage, and the cost for circumvention tool developers of staying ahead of China and other filtering countries may increase greatly, since signature-based blocking can be much more difficult to defend against.

Tool developers need to consider other problems in addition to blocking resistance. We were surprised at the relatively high error rates generated by many of the tools we studied. It is possible that some users do not care if the layout of webpages is broken so long as a YouTube video they wanted to access is viewable. But some layout errors render pages unreadable, especially pages in extended Unicode character sets. And the blocking of local sites accessed through circumvention tools opens a new front in the battle against circumvention tools.

If we consider the speed of tools as well as error rates, it's easy to understand why circumvention tools are not used universally. The fastest tools we analyzed require a substantial financial investment to access. The fastest widely usable free tool we analyzed takes 3.6 times as long to load the average page as an unblocked connection. (Again, times vary widely from page to page and from country to country—please look at standard deviations and at the individual country results as well as the top level mean score.)

Free tools that are not supported by ads are not without cost, of course. At current levels of investment, they are able to provide highly accessible services at speeds significantly slower than the uncensored Internet, and significant error rates in pages delivered. More investment may lower access times, but it may also make these systems targets for more aggressive attempts at blocking.

One intriguing finding in our data is that some tools perform very differently when tested in different nations. A few of the tools we tested performed poorly in South Korea, others poorly in UAE. It is possible that tool developers may be optimizing tools for use in China, Iran and other countries commonly associated with Internet censorship, and may be failing to consider the challenges of accessing censored content in South Korea. We hope to investigate further and see if we can confirm this finding.

Part of our intent with this study was to demonstrate that we could conduct circumvention tool testing on a more regular basis without physically traveling to the nations we wished to test. We can consider that experiment a partial success. We had a difficult time testing VPNs in most test beds, but we were able to test other tools without major problems. With VPSs in place, it is easier to perform tests on a regular basis, or on a specific day in response to reports that a tool was being blocked. If we did so, we would be able to offer near-real-time data on tool usability, rather than reporting on an annual or less frequent basis.

The limit to this new method is the availability of suitable VPS servers. We found usable platforms in five countries—we were only able to work in four countries due to US Treasury sanctions against Iran. Many VPS services market themselves within a given country but actually host their services in data centers outside of that country. Many VPS services only offer Linux based systems, which are only able to test a subset of circumvention tools. We found two VPS services in filtering countries for which we paid for service that was never set up—this behavior may have been simple fraud or it might have been because of suspicion of our use of the systems (we did not try to hide our identity when renting the VPS services). And the configuration of the VPS services to handle circumvention testing, particularly for VPN services, proved difficult or impossible in some cases. Despite these limitations, we were able to test more tools in more countries at lower cost than in our previous round of testing.

METHODOLOGY

To test the 17 tools we evaluated, we contracted with companies in China, South Korea, Vietnam and the UAE to rent Virtual Private Servers (VPSs) on a monthly basis. These four countries were the only countries that practice substantial Internet filtering (as determined by the OpenNet Initiative), that have companies that offer VPS services with Windows servers, and that are not under US Treasury sanctions. On each VPS, we installed each circumvention tool.

For each country, we generated a list of the twenty most popular sites in that locale according to Google Adplanner. We added those twenty popular sites to a list of up to twenty sites that ONI reported as blocked in the country in question. We verified that each of the blocked sites was still available from the U.S. and was blocked in the country.

To perform testing, we used Perl scripts that generated test scripts for the Selenium web testing application. The Selenium scripts instructed Firefox to connect to each site, record the time it took to load the entire site (including all images and other associated content, though not flash content) and verify that some piece of text specific to the site was present on the page. For every site requested by the testing script, the scripts saved a screenshot of the loaded page for later examination and verification of errors.

Where possible, we instructed the scripts to load a specific sub-page of each site. For instance, to test Facebook, we loaded http://facebook.com/Ashton and verified that the text 'live love laugh' (a snippet in the sidebar of Ashton's page) was present in the loaded page. For the simple web proxy tools, we used custom testing scripts to load each site using the in-browser interface for the tool. The script set a timeout of 3 minutes for loading each site, so 3 minutes is the longest time possible for any site/tool/country triad. When a set timed out, it was logged as an error only if the site didn't load enough data to pass the snippet text test.

We ran tests on each of the above tools on the VPS in each country and then ran the country script for each tool on each country's VPS. After running all of these tests, we aggregated the results into a single data set and cleaned the results by verifying all errors using the saved screenshots. We also removed any sites for which test testing did not work because the test snippet had gone bad between writing and running the tests.

The scripts ran for two test periods, one beginning in late February/early March and another in late March/early April.

The major problem with this method, as discussed above, was the difficulty in installing certain software within the VPS paradigm. VPN software often tries to make changes in network settings at a very deep level—these settings are often incompatible with a Windows server run as a VPS. In many cases, we ended up successfully activating the VPN, but in doing so locked ourselves out of the machine. In some cases, we were able to regain access through a persistent route to the VPS from a server in the US—in other cases, we were not. The "bad test" entries reflect cases where we were not able to use our methods successfully to test the tools.