CASTING A WIDER NET
LESSONS LEARNED IN DELIVERING BBC CONTENT ON THE CENSORED INTERNET

October 11, 2011

Canada Centre for Global Security Studies and Citizen Lab at Munk School of Global Affairs, University of Toronto
http://munkschool.utoronto.ca/downloads/casting.pdf
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>I</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>IV</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>V</td>
</tr>
<tr>
<td>- Key Takeaways</td>
<td></td>
</tr>
<tr>
<td>- Recommendations</td>
<td></td>
</tr>
<tr>
<td>1. Introduction</td>
<td>8</td>
</tr>
<tr>
<td>- The Shift Towards Online Broadcasting</td>
<td></td>
</tr>
<tr>
<td>- Global Blocking of International Broadcasters</td>
<td></td>
</tr>
<tr>
<td>- What Can News Broadcasters Do to Meet this Challenge?</td>
<td></td>
</tr>
<tr>
<td>2. Internet Censorship Detection</td>
<td>14</td>
</tr>
<tr>
<td>3. Circumvention</td>
<td>17</td>
</tr>
<tr>
<td>- Who Uses Circumvention Technologies?</td>
<td></td>
</tr>
<tr>
<td>- Propagation Strategies</td>
<td></td>
</tr>
<tr>
<td>4. Case Studies</td>
<td>23</td>
</tr>
<tr>
<td>- Background</td>
<td></td>
</tr>
<tr>
<td>- Introduction of BBC Web-proxy Services in Iran and China</td>
<td></td>
</tr>
<tr>
<td>- Measuring Patterns of Web-proxy Use</td>
<td></td>
</tr>
<tr>
<td>- 2010 Nobel Peace Prize Ceremony</td>
<td></td>
</tr>
<tr>
<td>- 2011 Tiananmen Square Protest Anniversary</td>
<td></td>
</tr>
<tr>
<td>- 2009 Iranian Election and Protests</td>
<td></td>
</tr>
<tr>
<td>- 2011 Anniversary of 2009 Iranian Election and Protests</td>
<td></td>
</tr>
<tr>
<td>- Propagation Strategies Across the Case Studies</td>
<td></td>
</tr>
<tr>
<td>- Case Study Takeaways</td>
<td></td>
</tr>
<tr>
<td>5. Alternatives to Providing Circumvention Services</td>
<td>52</td>
</tr>
<tr>
<td>- Limitations of Delivering Content through Web-Proxy</td>
<td></td>
</tr>
<tr>
<td>- Use of Content Delivery Networks</td>
<td></td>
</tr>
<tr>
<td>- RSS and Syndication</td>
<td></td>
</tr>
<tr>
<td>6. Summary and Recommendations</td>
<td>55</td>
</tr>
<tr>
<td>7. Areas for Further Research</td>
<td>58</td>
</tr>
<tr>
<td>8. Suggested Readings</td>
<td>60</td>
</tr>
</tbody>
</table>
FIGURES & TABLES

Table 1 Sample of blocked news organization websites  12
Figure 1 GeoStats interface  15
Figure 2 Barriers to accessing the uncensored Internet according to survey respondents  20
Figure 3 Login activity with no active propagation of the node (BBC Chinese)  21
Figure 4 Total number of web-proxy logins to BBC Chinese and BBC Persian services  26
Figure 5 Total logins to BBC Chinese radio web-proxy node  27
Figure 6 Total logins to BBC Persian social media web-proxy node  28
Figure 7 BBC Persian requests per login (weekly), July 2009 – July 2011  29
Figure 8 Introduction of a new node to replace a blocked node (BBC Chinese)  30
Figure 9 News stories and Chinese node usage, February – March 2011  34
Figure 10 Twitter node traffic shown with propagation tweets and retweets  36
Figure 11 Daily logins to BBC Chinese Web-proxy nodes  37
Figure 12 bit.ly usage graph of Persian proxy server  39
Figure 13 Persian nodes February – May 2011  42
Figure 14 Persian nodes June/July 2011  44
Figure 15 Persian email nodes June/July 2011  45
Figure 16 Persian email nodes May/June 2011  47
Figure 17 Activity on BBC Persian nodes July 2009 – March 2010  48
CASTING A WIDER NET: Lessons Learned in Delivering BBC Content on the Censored Internet

FOREWORD

The broadcasting of news across borders has been a perennial struggle and a heavily politicized arena of international relations since the first radio and television broadcasts of the early twentieth century. During World War II, the Nazis enacted strict laws to prevent German citizens from listening to foreign broadcasts, and distributed cheap receivers designed to prevent reception from far-off locations. Early in the Cold War, the Voice of America (VOA) launched a Russian language service targeting audiences inside the Soviet Union. Within a year, the Soviets reacted with an all-out intensive jamming effort employing over 750 transmitters that effectively crippled short wave reception of the VOA. Radio engineers at the US State Department responded with a massive “Ring Plan” designed to overwhelm the Soviet jamming technology with shortwave transmitters and a series of high-powered relays that encircled Soviet territory.

Today, contests such as these continue unabated, but they have migrated to a new medium of struggle: the Internet. That the Internet has contributed to massive explosion in the circulation of information worldwide, and a dramatic empowerment of individual liberty to access information and speak freely, are well established. But what is perhaps less well known is that many governments have become more capable at countering the flood and restricting speech online. At one time it was widely assumed the Internet would outflank and immobilize heavy-handed blocking attempts; now more than forty countries engage in some sort of Internet filtering. Many of them do so to restrict their citizens from accessing “foreign” news that may be critical of state policy or shed light on areas that leaders would rather leave in the shadows. China, Iran, Burma, Vietnam, Cuba and many other countries have filtered, at one time or another, access to the websites of news sites, both large and small. Some of the blocking efforts seem trivial in relation to the threat. For example, Pakistan recently ordered at least a dozen Internet Service Providers (ISPs) to block access to the website of the popular entertainment magazine Rolling Stone because of a news article that referenced Pakistani military spending.

The websites and Internet broadcasting platforms of the VOA (and its affiliated broadcasters, like Radio Fardi, Radio Free Asia, and Radio Free Europe) are persistent targets for Internet filtering by the United States’ main adversaries. Much like the “Ring Plan” of the Cold War, the US government has countered with the funding of software — firewall busting technologies — designed to route around or “circumvent” those filters. Over the last two years, the US Congress has put forward at least $45 million for the development and distribution of these circumvention tools (as well as training and local language support on how to use them) under the banner of its “Internet Freedom” agenda.

Not surprisingly, the US efforts have generated considerable push back. China’s censors have become extraordinarily adept at picking off and blocking connections to circumvention software connections through its “Great Firewall.” Vietnam was one of the first countries to make their possession and use illegal, and now Burma, Syria, and Iran do as well. Iranian leaders have not only made the distribution of circumvention technologies illegal and targeted them for disruption, they
have characterized them as part of a “soft war” against Iran. In light of US funding efforts for circumvention tools directed at Iran, it seems hard to disagree with them. As with the “cat and mouse” game of shortwave radio broadcasts of an earlier era, circumvention of Internet filtering is highly politicized and bound up with the projection (and protection) of national interests.

Regardless of the clashes of state interests, Internet censorship will present a growing challenge for broadcasters of all types today. Dozens of media websites and their products, from independent blogs to major global services, are now routinely targeted for censorship, disruption or regulation. As global news moves online, and content becomes subject to increasingly tight restrictions in numerous national jurisdictions, the challenges of delivering content to target audiences are becoming increasingly complex. To succeed internationally, broadcasters will need to develop a comprehensive strategy to navigate this new media terrain carefully.

The aim of *Casting a Wider Net: Lessons Learned in Delivering BBC Content on the Censored Internet* is to help develop just such a strategy.

*Casting a Wider Net* is the first in what we hope will become a series of major research reports on security sponsored by the Canada Centre for Global Security Studies at the Munk School of Global Affairs, University of Toronto. The Canada Centre for Global Security Studies has several unique strengths and aims, all of which are represented in this report. The research undertaken in *Casting a Wider Net* represents a collective effort of several individuals and organizations from the public and private sectors, and reflects primary field research and technical analysis undertaken by experts in multiple scholarly disciplines.

Karl Kathuria, the primary author, led the research while on secondment from the BBC as the Canada Centre Visiting Fellow in Global Media (2010-2011). He worked closely with several researchers at the University of Toronto’s Citizen Lab with expertise in the social sciences and data analytics and visualization. The data from which *Casting a Wider Net* draws includes traffic statistics from the BBC’s Internet operations, research on Internet controls undertaken by the OpenNet Initiative (a collaboration among the Citizen Lab at the Munk School of Global Affairs, University of Toronto, the Berkman Center for Internet & Society at Harvard University, and the SecDev Group), and data shared by Psiphon Inc., a private company born at the University of Toronto’s Citizen Lab and now one of the world’s leading providers of circumvention services. The report’s synthesis and analysis of these and other primary data sources makes it a unique and original contribution to the study of Internet censorship and circumvention.

*Casting a Wider Net* also makes several important substantive contributions: It provides an extensive analysis of tradecraft in the area of circumventing Internet controls - what works, what does not, and why? *Casting a Wider Net* urges broadcasters to be pragmatic in their choice of methods, using the entire tool kit instead of relying on a single tool, to deliver content into censored jurisdictions. It provides some counter-intuitive findings, including that major events on the horizon in the case studies under examination did not lead to anticipated increases in blocking, while some other unanticipated events did. This experience leads to one of the report’s most important recommendations: broadcasters must be agile and alert to new circumstances. Blocking events
can be unpredictable, and so broadcasters need as close to real-time situational knowledge as possible of not only their own traffic status but that of the national networks within which their audience resides.

Lastly, *Casting a Wider Net* reinforces what is becoming increasingly understood by Internet scholars and policymakers alike: the challenges presented by growing Internet controls worldwide cannot be solved by a single tool or a “silver-bullet” software solution. What is required is a comprehensive, multi-pronged strategy based on a thorough understanding of the situation on the ground. We hope *Casting a Wider Net* provides broadcasters with the basis for such a strategy moving forward.

**Ronald Deibert**
Director, the Canada Centre for Global Security Studies and Citizen Lab
Munk School of Global Affairs
University of Toronto
ACKNOWLEDGEMENTS

The Canada Centre for Global Security Studies is an interdisciplinary unit at the Munk School of Global Affairs, University of Toronto, that engages in advanced research and policy development around global security issues including cyber security, global health, and region-specific concerns, such as the Arctic, Europe and the Commonwealth of Independent States, Asia, and the changing face of the Americas.

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, at the University of Toronto, focusing on advanced research and development at the intersection of digital media, global security, and human rights. The research of the Citizen Lab is supported by a generous grant from the John D. and Catherine T. MacArthur Foundation.

This report represents a collective research effort based at the Canada Centre and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The primary author and project lead was Karl Kathuria (BBC and Canada Centre for Global Security Studies). Masashi Crete-Nishihata (Citizen Lab) provided written and analytical inputs. Greg Wiseman (Citizen Lab) led data analysis and visualization. Ron Deibert (Canada Centre for Global Security Studies and Citizen Lab) provided guidance and editorial oversight. Jacqueline Larson provided editorial assistance. James Tay (Citizen Lab) and Adam Senft (Citizen Lab) provided research support. Jane Gowan (Citizen Lab) produced the cover and layout design.

We are grateful to Psiphon Inc. for sharing their traffic data to the Canada Centre and Citizen Lab research team, and the BBC and the SecDev Group for sharing their private report on circumvention use in Iran. Several individuals at the BBC provided helpful support and assistance. We are grateful to Frank Ip for his input, Anne Barnsdale and Roxanna Shapour for reviewing the report, and Mateusz Pawlowski and Jamie Dale for providing information on the BBC’s Geostats project.

Casting a Wider Net is an independent research activity of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto.

The views expressed in this report are those of the research team only, and do not represent the official position of the BBC, Psiphon Inc., or any other third party.
EXECUTIVE SUMMARY

The Internet has changed the world of news broadcasting. International news broadcasters increasingly rely on the Internet to deliver content to their audiences, who are often in multiple national jurisdictions. However, Internet controls are growing worldwide, with many countries actively blocking news and other websites from reaching their citizens. The British Broadcasting Corporation (BBC) delivers international news content in 27 languages in addition to English. An increasing number of these localized language services is delivered into countries that implement some form of Internet censorship.

This report analyzes a pilot program the BBC conducted to provide web-proxy services in China and Iran where Internet censorship is pervasive and localized BBC language content has been consistently blocked. Web-proxy nodes enabled users to bypass censors and connect to BBC content. The nodes were propagated to audiences through a variety of channels including on-air broadcasts, social media, and email newsletters. This report outlines the findings of the program and focuses on a series of case studies in Iran and China around sensitive political events that were likely to trigger increased censorship from authorities.

The report shows that bypassing Internet censorship to deliver news content in restrictive communications environments involves far more than just supplying circumvention tools. Broadcasters need to devise a strategy for distributing content over the Internet with an understanding of the different challenges they will face in each of the target countries they are trying to reach. The following key takeaways and recommendations summarize the findings of this report, and share lessons learned to help international broadcasters formulate delivery strategies when their content is blocked online.

KEY TAKEAWAYS

Bypassing Internet censorship requires a new approach to content delivery

Reaching audiences in restricted environments through circumvention technology represents a new delivery platform for news media that requires infrastructure, investment, and strategic thinking from broadcasting organizations. Any circumvention tool should be treated by the broadcaster like any other distribution platform would be, as a way of reaching its audience, and thus avoiding the political connotations of the word “circumvention”.

Blocking events are unpredictable and require agile reaction from broadcasters

Blocking events can be unpredictable, and often occur when news stories break. By reacting to blocks with web-proxy services, it is possible to experience only a minor break in service, as long as replacement nodes are available and quickly propagated. Trust is important; broadcasters need to make sure the service they offer is both technically reliable and always accessible to an audience.
that is reaching out for news and information.

Real-time blocking detection is essential

To react in a timely and effective manner to blocking events, news broadcasters require as close to real-time detection of service blockages as possible. There are different blocking methods depending on the country, so any real-time alerts need to be verified, but in each case there will be sudden drop-offs for traffic to websites or proxy servers. By reacting quickly to these blocks, broadcasters will minimize the time in which its service is unavailable.

Content needs to be reusable

If a broadcaster is making its content available through only one URL the effect of potential blocking can be greater. Syndication of content, and distribution through multiple content delivery networks, can help make content blocking more difficult by increasing the number of URLs associated with it, and effectively “hiding” content in other locations.

Propagation strategies should be diversified

Each method of propagating a web-proxy service can be considered a “channel” for distribution. The URL that is promoted on air should be different from that sent via email newsletters, which in turn should be different than the URL promoted via a social media channel such as Twitter.

Each method of propagation has its own strength

Different methods of web-proxy propagation have particular strengths. Twitter is useful for short-term boosts in usage, but will also likely increase the number of logins from outside the target country. During the pilot study email newsletters and promotion over traditional broadcast media did not result in the same level of usage peaks but helped grow audiences steadily. While direct communications with links to private nodes can be effective for reaching a core audience that trusts the service, audiences will also pass the message around themselves, either by forwarding on messages or through direct word of mouth. Getting the message to the audience in the first place is likely to be a catalyst for further dissemination.

RECOMMENDATIONS

Be clear about objectives

Broadcasters need to clearly define what they hope to gain from providing Internet censorship-circumvention services to audiences. The objective of the circumvention strategy outlined in this report was to deliver content to audiences in countries where blocking is pervasive and has a negative effect on the accessibility of BBC content. However, the provision of only circumvention software may not necessarily achieve this objective. Broadcasters may also benefit from combining circumvention technologies with adaptive content that can be carried through other websites and media channels.
New delivery platforms require commitment and investment

Investment in this new delivery platform needs to be ongoing and will increase the overall distribution costs associated with Internet content delivery. Circumvention tools tend to have a higher cost-per-user associated with them than delivery of content over the open Internet, because of the additional costs stemming from the management of what is effectively a bespoke delivery platform.

Be adaptive

There is no single technique or tool for ensuring content delivery in restrictive environments. Broadcasters need to explore multiple tools and delivery strategies, and adjust to shifting requirements and challenges.

Internet censorship is dynamic and can vary significantly between countries and regions. Broadcasters need to adapt to different environments and be able to implement strategies that address shifting requirements and challenges. Effective delivery strategies must consider technical variance in filtering, the political climate that enforces censorship regimes, and the social nuances of the audience the news is trying to reach. The broadcaster must also consider the responsibility it has to the user, by adapting its strategy to account for users’ security (which can vary depending on locale), making sure that they are aware of the risks associated with accessing such content.

Collaborate with stakeholders

Individual news broadcasters will have different strategies and objectives for providing circumvention services. However, by working together to address the issue of content delivery in restricted markets, news broadcasters will have a better understanding of restrictions, and will be able to use common approaches.

Broadcasters should also consider collaboration with stakeholders from academia and the private sector. Broadcasters can bring their own in-depth knowledge of the broadcasting environment to academics who are studying Internet censorship, and other organizations who are trying to deliver content into restricted markets. Sharing information for research and public education will improve understanding of the problems that companies and individuals face in distributing information and participating freely online.
1. INTRODUCTION

The nature of news broadcasting has changed dramatically in recent years, particularly for organizations offering international services to global audiences. The Internet era has introduced more than just a new technology for media delivery—it has brought the world together like no other existing platform, allowing people to communicate and collaborate. It has paved the way for individuals to contribute to news stories and report them in their own way to a potentially huge audience with very low entry costs.

While larger broadcasters are still needed to collate, organize, and report the news in a coherent, trustworthy way, they also need to work with people on the ground and contribute to the global conversation. Peter Horrocks, Head of Global News for the BBC, articulated this change in emphasis when speaking to the 2011 International Journalism Festival:

“In the age of the Internet, is there any need for a news organization to aspire to do what the Internet itself can do – be both the source and the distributor of the news?”

“There is no doubt that the Internet, whatever the debates about how it undermines business models, is brilliantly conceived for news. It is inherently open to free information and perspective, the life-blood of news.

The BBC certainly doesn’t see the Internet as a competitor. Instead we exploit its every advantage and try to make sure that we respond to its challenges.”

While the Internet provides rich new possibilities for the production and dissemination of news media it also presents significant challenges for news organizations.

Early debates on Internet regulation included the popular argument that geographically based legal regulations did not apply, and therefore cyberspace could not be controlled by nation states. However, in recent years it has become clear that the Internet is not the unfettered space it was once thought to be, as states around the world are actively seeking to shape and control the flow of information online. A common practice for achieving such control is filtering Internet content to prevent citizens from accessing certain information.

Internet censorship has become a growing and pervasive global trend. The OpenNet Initiative (ONI) has been documenting the prevalence of Internet censorship and information controls in countries around the world for nearly a decade. In 2003 when the ONI started tracking Internet censorship, only a handful of countries filtered online content. Today over forty countries implement some form of content control over the Internet. Restricting the flow of information online is practiced by authoritative as well as democratic regimes. These increasing controls have created national boundaries in cyberspace that mirror the borders of the physical world.

For broadcasters that operate multilingual international services, such as the BBC, Broadcasting Board of Governors (BBG), and Deutsche

1 “Peter Horrocks: Becoming More Global,” BBC Press Office, 14 April 2011, full source link http://....

Welle, target audiences will be based in multiple countries, and the services will often aim at individuals in states where authorities have set up borders in cyberspace that restrict the free flow of information. Audiences behind these barriers are a relatively small proportion of the global audience for broadcasters, but are likely to be an influential niche that may potentially grow into a mass audience in the future. This audience will be vital for broadcasters who wish to remain relevant to a changing audience.

The objective of this report is not to examine what role news broadcasters need to play in the relatively new environment of cyberspace to compete editorially. Instead, it takes the starting point that news broadcasters are aiming to deliver their services over the Internet, whether via websites, audio, or video, and that they are trying to reach a large global audience. With this frame in mind, the report focuses largely on the technical distribution of web content into restricted markets. To respond to the challenges of delivering content over the Internet, news broadcasters will need to respond to events where their sites and content are blocked.

This report uses the BBC as a case study to explore the challenges facing news broadcasters in delivering services to restricted environments. The countries under focus are China and Iran, where the BBC has faced problems in distributing web content for many years and in response has experimented with propagating links to web-based proxy servers to help target audiences reach its content in countries under Internet censorship.

As well as looking at the longer-term impact of circumvention services, the report considers the impact of short-term blocking events, both actual and predicted, and the growth of services using particular methods of propagation. The report’s findings inform a broad strategy for how broadcasters can achieve their goal of reaching a global online audience with content that may be at risk of being filtered or otherwise blocked.

**THE SHIFT TOWARDS ONLINE BROADCASTING**

Major broadcasting organizations are increasingly moving from traditional news media and infrastructures to online platforms. In the 2010 UK Government Spending Review, the Chancellor cut the BBC World Service’s budget by 16 percent over four years, and changed its source of funding from a Foreign and Commonwealth Office grant-in-aid model to license fee funding from 2014. Peter Horrocks responded to this change by announcing the likelihood of significant job losses and the closure of several radio services because the BBC needs to change its focus for delivering content with a much lower budget.

The international strategy for the BBC’s Global News Division has a heavy reliance on delivering its services digitally, with language output in some cases being moved away from traditional broadcasting platforms into the Internet environment. In the Global News Objectives for 2011-2012, the BBC makes explicit its aim to “increase digital growth to become the world’s leading digital news provider.”

Other international broadcasters are facing similar challenges in the shifting nature of news broadcasting. According to the US-based BBG’s “Technology Strategic Plan and BBG Technology Update” covering 2010-2012, one of the key challenges for the current period is in the declining effectiveness of its shortwave broadcasts. The report acknowledges that “as the population in...”

---

most countries has continued to migrate its media consumption to other technologies (AM, FM, TV, satellite radio and TV, mobile phones, and the Internet), the cost effectiveness of shortwave transmissions continues to wane and is expected to be circumscribed to a very small number of target countries in the relatively near future.”

The shift towards online broadcasting and new media for news broadcasters is not without its own challenges. In comparison to radio and television broadcasting, the number of people viewing news content online is relatively small. The BBC announced a total global audience of 225 million people in 2010-2011, 166 million of which accessed content from BBC World Service (i.e., more than half), and 13 percent of the audience accessing its services online. This shift in focus is not unique to audio/video broadcasting. Amidst heavy financial losses, the Guardian Media Group has begun a policy of what it calls “digital first,” accompanying a plan to double its digital revenues by 2016.

There is clearly a potential for growth in delivery of services online, and many organizations are claiming that the increased use of mobile devices will offer further opportunities to reach audiences and, ultimately, increase revenues. According to Cisco’s Visual Network Index, mobile data traffic will have a compound annual growth rate of 92 percent between 2010 and 2015, which is a three times faster growth rate than fixed IP traffic. Broadcasters are keen to exploit this new, fast-growing market, and are developing both applications and services with this objective in mind. For example, the BBC reported in 2010 that 5 percent of its online audience was in Nigeria; the BBC is adopting its international strategies to make sure its services are available on platforms relevant to its audience.

Broadcasters’ and other global organizations’ digital strategies seem to rely on unfettered transmission over the Internet in which content is delivered in the same way to all countries. While the BBC’s delivery relies primarily on content distribution using a mixture of its own infrastructure and Content Delivery Networks (CDNs), BBG has for a number of years recognized that its content delivery has been compromised, and has developed strategies and technologies to deal with these compromises.

The BBG’s “Technology Strategic Plan and BBG Technology Update” recognizes the importance of developing strategies to bypass censorship and blocking of its content:

New media figure prominently in BBG strategy despite current, low audience numbers, as global trends point to progressively higher take-up rates among key demographic segments. BBG new media services must be increasingly sophisticated, targeted, and competitive – on the understanding that interference by repressive governments can thwart our best efforts.

In a recent interview, Ken Berman, BBG’s Chief Information Security Officer and director of Internet freedom programs, said “our idea is that an educated citizenry, if they get all the news and views, should be able to make up their own minds. The deeper mission of this program

---

5 “BBC World Service Audience Drops after Cuts,” BBC Press Office, 12 July 2011, full source link http://....
7 “Visual Networking Index,” Cisco, full source link http://....
8 “BBC Online – Our Mobile Future,” BBC Internet Blog, 17 February 2010, full source link http://....
is to encourage freedom of inquiry and freedom of information.”10 In the same interview he also explained the importance of his efforts to reach an audience on the Internet, by pointing out that less than 1 percent of Chinese citizens listen to shortwave broadcasts, while there are more than 380 million Internet users.

Delivering content online poses a new set of challenges for broadcasters. A delivery strategy for radio services may involve a combination of shortwave, medium wave, and FM broadcasts, and television services can be delivered over satellite, cable, or terrestrial broadcasts. Delivery of content over the Internet will also require a combination of different types of technology:

- **Infrastructure** — Web content can either be hosted directly by the broadcaster using its own infrastructure, or using a combination of CDNs.

- **Circumvention tools** — For countries or regions where the content is being blocked, the broadcaster can decide to either provide circumvention tools itself, or to help its audience in other ways by pointing them at circumvention tools that are already available, and guiding them toward methods of consuming the online content.

- **Third-party delivery** — The broadcaster may need to adapt the way its web content is structured and developed, making use of technologies such as RSS feeds for syndicating news and information through sites and blogs owned by other organizations and individuals.

In some cases, the delivery method may dictate the capacity to provide extended functionality within the site. Some multimedia elements and scripts may not function over circumvention software or syndication methods. The broadcaster then needs to prioritize its content and choose a method of delivery that allows it to bypass censorship.

**GLOBAL BLOCKING OF INTERNATIONAL BROADCASTERS**

Internet censorship poses significant challenges to broadcasters that have invested time and resources in creating content for online audiences that it cannot reach because their websites are blocked. The BBC has faced challenges in delivering content to both China and Iran where localized online services have been subject to pervasive blocking for many years. However, beyond these two examples, the challenge of Internet censorship is a widespread issue affecting a number of target markets and news organizations. Table 1 shows the availability of news media websites based on data from an ONI Internet filtering testing sample from 2010-2011; an x indicates the organization has at least one of its web pages blocked in the respective country. All of the countries listed in the table block English content from international broadcasters and several (Burma, China, Iran, and Vietnam) target media content produced in the local language. This sample is a limited snapshot of global blockages, but shows that the challenge is not unique to the BBC or the countries analyzed in this report.

---

WHAT CAN NEWS BROADCASTERS DO TO MEET THIS CHALLENGE?

To ensure content delivery to target audiences in restrictive environments broadcasters need to help their users bypass content filters. However, providing effective strategies for audiences to evade Internet censorship requires more than simply offering circumvention software.

Taking the step to distribute or promote circumvention tools can be considered a controversial move by a large news media organization. In providing software, the supplier has a duty of care to the user. If a broadcaster is to host and distribute circumvention software, it needs to ensure it does so in a way that meets technical, legal, and ethical requirements.

A broadcaster may make the decision to provide such software, or it may link to existing technologies with a clear message to the audience that it provides no warranty in doing so. Alternatively, it may adopt other strategies for bypassing censorship, such as working more closely with partners by syndicating its content, either through formal agreements or making its content available for bloggers and other site
owners to pick up and distribute on the broadcaster’s behalf.

Whatever technologies and tactics are utilized for circumventing Internet censorship, the broadcaster needs to adopt a strategy that can fulfill its primary objective of delivering news content to its audience. While the implementation of these strategies will differ depending on the country involved, the basic principles will be the same. There are three areas in which the broadcaster can be active:

1. **Detection of blocks**
   
   It is vital for any global organization to know when delivery of its content is being compromised. A number of different tools and methodologies exist for detecting Internet censorship and section 2 summarizes a few approaches. That section also describes a software prototype developed by the BBC to detect blocking of its own content, and discusses how this prototype could be provided to a wider audience and other organizations.

2. **Provision of circumvention tools**
   
   There are many circumvention tools available, some of which are more suited to broadcasters than others. This report includes case studies based on the BBC’s experience in providing web-based proxies for distributing its content in China and Iran, looking at why methods were chosen, and how effective its propagation strategies have been for introducing software to its audience.

3. **Audience education**
   
   Providing circumvention software is only part of what a broadcaster can and should do to help its audience. A broadcaster needs to know that the audience is aware of the problems they are facing and knows that there are ways of accessing news content despite blocks and filters. The broadcaster should also educate its audience in how to access content safely, and make sure they are informed of any possible legal dangers in accessing the broadcaster’s site. Finally, it needs to make its audience aware of how to bypass censorship.

The case studies in this report show the need to continually refresh the message while building up an audience in countries facing these problems.
2. INTERNET CENSORSHIP DETECTION

Accurately detecting and verifying blocking events in a timely fashion is vital for international broadcasters delivering content into restrictive environments.

Internet content filtering is implemented in a number of different technical, legal, and political forms. It is a dynamic process, which can shift rapidly and often unpredictably. Rigorously monitoring these changes requires attention to both technical and political dimensions.

The ONI has been documenting Internet censorship since 2003 and has tested for evidence of filtering in seventy countries and on 289 ISPs. The ONI uses a simple technical methodology to verify Internet censorship. Lists of websites and keywords are collected that cover topics that might be targeted for censorship including pornography, gambling, international and independent news media, human rights, and political content. A data collection software client designed to query these pre-defined lists of URLs is distributed to researchers within countries suspected of engaging in Internet censorship. The list of URLs is accessed simultaneously over HTTP both in the country suspected of Internet filtering and a country with no filtering regime (e.g., Canada). The data gathered from the country with no filtering is used as a control to compare the data from the country suspected of filtering. Where appropriate, the tests are run from different locations to capture the differences in blocking behaviour across ISPs.

Other approaches have focused on monitoring the technical practices of particular filtering techniques such as the system developed by the Chinese government. Herdict Web is a project that provides a publicly accessible web interface that enables users to report inaccessible sites and generates visual aggregates of these reports. This crowd-sourcing approach can provide real-time reports of potential blockages, but relies on user-submitted reports, which may produce false positives, such as mundane network errors mistaken as censorship.

Research projects such as the ONI, Herdict, and related efforts can provide broadcasters with an overview of filtering practices in different markets and relate technical information and contextual layers that may help organizations understand why and how their content is blocked in particular jurisdictions. However, reacting to blocking events effectively and providing mitigation options for affected audiences requires precise real-time data on potential service blockages.


In 2010, the BBC recognized this need, and technicians from BBC World Service developed a software prototype — GeoStats — designed to detect and report when BBC websites are blocked. The system was partially inspired by Google’s Transparency Report, which provides information about the accessibility of Google products in different countries based on traffic data.14

GeoStats processes traffic data from two sources: BBC Livestats logs and Akamai (the content delivery network) logs. Traffic is aggregated hourly and by country, and then compared to previously seen data. Traffic below a certain threshold of the expected value would be flagged as a potential blocking event, and could be manually examined along with supplementary data sources, such as news reports or other contextual information (Figure 1).

GeoStats was developed as a proof of concept (i.e., a demonstration in principle), and during
development a number of shortcomings were identified. Many of these issues are attributable to the fact that the project was not fully financed, and was a lower priority than the team’s primary activity of Internet content distribution. One of the greatest lessons from the system’s development was that the data needs to be as close to real-time as possible. Akamai log files could be delivered up to twenty-four hours after the event, and Livestats data was closer to real-time but only sampled. This meant that the system could miss the blocking events, making the BBC unable to react to the blocks in a timely manner.\(^\text{15}\)

---

\(^{15}\) For a detailed description of GeoStats, see Karl Kathuria, “Bypassing Internet Censorship for News Broadcasters,” Paper presented at the USENIX Workshop on Free and Open Communications on the Internet (FOCI ’11), San Francisco, CA, 8 August 2011, full source link http://...
3. CIRCUMVENTION

The majority of circumvention tools fall into three general categories: client-side, virtual private network (VPN), and web-based. While all of these approaches can be used to circumvent filtering, they each have features that may make them more or less suited to deployment by news organizations.

A VPN is a computer networking method that encrypts and tunnels Internet traffic through a proxy location. VPN use has risen in recent years and become more user friendly through simpler configuration of PCs using recent operating systems. VPNs are also readily available to buy, either for commercial gain or for political motives. A survey study commissioned by the BBC on circumvention users in Iran found that VPNs were often believed by web users to be dangerous and possibly government controlled. One respondent referred to a television program called Marzhaye Shishei (“Glass Borders”), in which IT experts warned against buying from unknown companies and using circumvention tools.

While VPNs can be challenging to set up for non-technical users, and are not necessarily perceived as trustworthy, they tend to be fast and are usually able to access all content on websites, including JavaScript and audio/video. For a news broadcaster, it is the latter benefit that makes the provision or support of VPNs particularly appealing because multimedia news content is usually a core offer.

Client-side software comes in many guises, with tools such as Tor, Ultrasurf, and Freegate being among the most popular. These tools have been promoted by some international broadcasters, such as the BBG. However, broadcasters should consider that promoting software implies a level of support for the product. Because the software itself also needs to be installed or run on the user’s machine, users may experience technical problems with installation or may have the software itself blocked on their machine if they do not have the required privileges to run executable code.

VPNs and client-side software are often provided for commercial gain, and not all operators of these solutions will be providing their software just for accessing news content. One reason for the lack of trust in VPNs is that financial transactions required to purchase VPNs can create links between the subscriber and the provider, and this information could be open to interception.

While the broadcaster may broadly support the use of any tool from which the end user can access its content, it may be less willing to provide third-party software directly for these reasons. With these considerations in mind, the main advantage of a web-proxy is that it can be accessed via a single URL. Since the web-proxy may still be controlled by a third party, it is easier for the broadcaster to point its audience to a proxy than to instructions for downloading software or configuring VPNs.

Although URLs to web-proxies can be and often are easily blocked, alternative URLs can soon be released, and again propagated through the broadcaster’s various channels. But the quick
turnaround and ease of access for web-proxies does come with a major disadvantage. As with many client-side solutions, web-proxies are often unable to handle rich media content, such as JavaScript and Flash audio/video. However, the use of web-proxies can also lead to marked success in building audiences. For example in February 2011, Radio Farda announced that they had experienced 8 million page views through their proxy servers.17

The BBC chose Psiphon Inc. as a provider of circumvention tools in reaction to news events in Iran during the June 2009 presidential election. Having evaluated various tools prior to this, the BBC considered Psiphon the “best fit” for its objectives. Without a specific budget available for bypassing censorship, there could be no development of new tools by the BBC itself, and no additional support burden for whatever the BBC would provide. Of the “off-the-shelf” solutions that were available, Psiphon was considered the most appropriate for the following considerations:

- **Usability** — The BBC would direct its audience to the tool, but could not be involved in supporting users of the software. Therefore, the solution had to be simple for its non-technical audience. A web-proxy, such as Psiphon, could be easily promoted via a single URL, with a user experience similar to browsing existing BBC websites. The users’ behaviour and experiences need not be significantly changed when they were accessing content through the circumvention service.

- **No executable code** — The BBC was not willing to provide software that had to be installed on the user’s PC. This decision was made for two reasons. First, supplying executable code from its website would imply that the BBC was responsible for the individual’s installation of the software, and any support they would require in using it. Second, the BBC’s objective was to enable users to access its site—it was not attempting to distribute software on a large scale for censorship circumvention or anonymity. The BBC would promote the web-proxy as an alternative way for audiences to reach its content only.

- **Informed use** — Efforts needed to be made to ensure users had appropriate information on the use and terms and conditions of circumvention software before using the provided service. This information was available in the form of a disclaimer on the Psiphon node’s login screen, explaining in simple language what the software was and how to use it, warning that it was not a tool for increasing individuals’ security or privacy, and providing a full list of terms and conditions.

- **Hosting environment** — The service had to be hosted in a secure environment, provided by a trusted corporate entity, and not be peer-to-peer based. Due to the responsibility the BBC has to its audience, and its reputation as a trusted global brand, it needed the assurance that the service was secure and reliable. Beyond the software’s functionality, the nodes’ continued running in a secure data-centre environment gave the BBC confidence that it could point its users towards Psiphon.

- **Exit strategy** — If the circumvention service was compromised in any way, or the BBC needed to withdraw from providing the service, then there had to be a way to do so immediately. Psiphon’s hosted solution could be stopped at any point, and access to the servers via the published URLs could be terminated.

WHO USES CIRCUMVENTION TECHNOLOGIES?

Circumventing Internet filters to deliver news content to restrictive communications environments requires an understanding of the target audience and how they use and perceive circumvention technology.

In 2011, the BBC commissioned a private research report into the Iranian market, to assess who uses proxy servers, how they do it, and why.\(^{18}\) The report is limited in scope because it was based on self-selecting questionnaires disseminated through Psiphon proxy servers provided by both BBC and Balatarin — a popular Iranian web forum. Despite this bias, the results of the study provide some insights into an audience that uses circumvention tools. The study is based on Iranian respondents. While the profile of the users may differ in China and other countries, some of the concerns and reasons for using circumvention services are likely to be similar.

The majority of respondents to the survey were male, under forty, and university educated to a bachelor-degree level or above. Although prior BBC research has shown that 39 percent of the weekly BBC Persian audience is female, 84 percent of the circumvention tools’ users in the survey responses were male. Ninety-seven percent of respondents either agreed or strongly agreed that unmonitored and uncensored access to the Internet is a universal human right. Respondents reported using circumvention tools for accessing filtered news and for chatting online with friends and family.

Figure 2 (next page) outlines four main barriers to accessing the uncensored Internet according to survey respondents. These results show that one of the greatest concerns for Iranian users is fear of being caught by authorities. Over 80 percent of respondents believed that Internet use is monitored in Iran. There is a high awareness of surveillance among this group, and for good reason: as well as direct surveillance of activities in public locations, the government requires ISPs to keep users’ traffic details for up to six months, keeping people mindful of the threat.

With these problems in mind, it is vital that a circumvention service can be trusted by the end user. Users of circumvention tools can often be suspicious of the software’s source. For example, one respondent to the BBC survey put it like this: “You think people don’t know that you are the Islamic Republic, and the Islamic Republic is you? Your intentions from this survey are completely clear.” The underlying suspicion and mistrust respondents seem to have towards circumvention presents an opportunity for news broadcasters who can educate their existing user base in the use of circumvention technology and guide them to the tools they provide. The trust that already exists between the user and the broadcaster can help to overcome this particular barrier, while provision of circumvention tools and education in their use can also help to raise awareness of the growing problem of content restrictions to its global audience.
PROPAGATION STRATEGIES

Broadcasters utilizing web-proxies to ensure media delivery in restrictive environments require a means to disseminate information about the service to users. A number of strategies can address this goal. The general approach for propagating nodes that is recommended by Psiphon Inc. is to promote one node on each available “channel.” For news broadcasters, this strategy requires having a number of nodes available at any one time, each of which needs to be promoted in one channel, and then monitored for its availability and reach.

Channels the BBC utilized for node propagation included:

- **Broadcast media** — Promoting the availability of circumvention tools and the URL of blocked BBC websites on radio and TV broadcasts.

- **Social media** — Occasional or regular messages advising that a node is available, with a link to it embedded in the message. The hope is that these get passed to a much wider network of people than the original subscribers to the broadcaster, for example, through retweeting messages over Twitter.

- **Email newsletters** — Regular emails distributed to audiences with marketing information or news updates and links to web-proxy nodes.

Regardless of the propagation method, the message can be “softened” so that it is not actively promoting software for circumvention. For example, in China and Iran the BBC disseminated a message noting “If you are having trouble accessing our site, you can try [node name].” This message does not suggest that the broadcaster is pushing circumvention software to the audience, but rather is merely trying to advise...
that its content is available through a channel other than its own website. Sending out the message in this way also shows that the broadcaster considers its circumvention platforms to be part of its content delivery strategy rather than a tool for mitigating general censorship.

Additionally, URLs can be shortened, using services such as bit.ly and tiny.cc. The use of URL-shortening services complements the propagation channels by providing more immediate statistics and giving an additional reference point for traffic. Using URL shorteners gives the broadcaster a near-real-time look at how many people are accessing the promoted URL for the service, which can then be cross-checked with people logging in to the proxy server.

Because web-proxy nodes are likely to be blocked eventually in censored jurisdictions, the broadcaster should have a procedure for bringing new nodes online and propagating that message to its audience. In the case of Psiphon, users can register and will be alerted when a node is blocked, and when its replacement is brought online. Figure 3 shows a period following the blocking of a node for BBC Chinese that was propagated through email newsletters. During this period there was a flurry of activity at the start, but no further propagation of the node, which led to a drop in activity. Conversely, there is a danger that too much promotion will attract the attention of authorities and the node will be blocked.

When a broadcaster addresses blocking of its content, it needs to be aware that it is not just attempting to provide access to its own content hosted on its own site. When a broadcaster evaluates propagation tactics, it should also consider how it can distribute its content through unfiltered sites.

The technical ability for third parties to carry web-based content has always existed, but it is
up to the broadcaster to make such content easy and appealing for users to access. This requirement may mean a shift in the broadcaster’s strategy so that it can make partnerships with other news providers, and push its content directly to them. Peter Horrocks told the International Journalism Festival in 2011, “we can no longer do it within our own walls. We need to network with our audience and we need to network with partner news organisations. We can no longer be fortress BBC. And that requires some dramatic changes in our mindset.”19 This shift in editorial focus, combined with the technical delivery of content, will make news services editorially stronger and more widely distributed, which in turn will make them less susceptible to blocking events.

The BBC’s international services already have partnerships in place with other news organizations but it needs to continue to build these partnerships and make their content more widely distributed. As well as commercial business-to-business deals, the use of widgets and public RSS syndication can help with distribution of content via indirect channels. These issues are discussed in more detail in section 5.

19 “Peter Horrocks: Becoming More Global,” BBC Press Office, 14 April 2011, full source link http://...
4. CASE STUDIES

This report presents four case studies, two each in China and Iran. The first case study for each country examines a situation in which a news event led to a surge in web-proxy use just after the service was first introduced. The second case study considers a specific point in time where the risk of blocking was considered high due to approaching anniversaries of sensitive political events. In each study, the report considers the events surrounding the propagation of web-proxies, and the impact of the different propagation strategies in reaching the audience.

BACKGROUND

Iran and China maintain two of the world’s most extensive Internet filtering systems and restrictive information environments. The Chinese government concentrates Internet filtering on content that could potentially undermine the government’s authority and its control over social stability. Similarly, the Iranian government primarily targets political content and material that is perceived as offensive to the standards of Iran’s religious leadership.

China conducts Internet filtering through a number of techniques including IP blocking, DNS tampering, and keyword filtering. A unique feature of Chinese Internet censorship is keyword filtering implemented at the backbone level. Targeted keywords include content related to sensitive historical events, controversial groups, and other topics the government deems taboo. This technique inspects the content of IP packets to determine if censored keywords are present and, if they are detected, sends reset packets to both the source and destination IP address to disrupt communications. This form of censorship presents users with a network timeout page that can appear to be the result of mundane network errors rather than intentional blocking. This system’s implementation at the backbone level means that the level and depth of censorship is consistent across Chinese ISPs and content can be quickly and uniformly blocked across the country.

In Iran, Internet filtering is implemented at the ISP level and is augmented by a centralized system that routes all public Internet traffic through proxy servers. All commercial ISPs in the country that offer Internet connectivity services are mandated to connect through the state-controlled Telecommunications Company of Iran, which provides a central point of control for authorities to conduct censorship and surveillance. Unlike users in China, users in Iran are presented with a block page when accessing censored content that warns them the website is prohibited.

Both countries aggressively block foreign news and independent media websites. This filtering targets both English and localized language services. The twenty-four-hour news site for BBC Chinese (http://www.bbczhongwen.com) was launched in 1999, and was immediately blocked by Chinese censorship authorities. The BBC Persian service (http://www.bbc.co.uk/persian/) was launched in 2001 and began to provide twenty-four-hour news in 2002. The service was blocked for the first time in Iran in 2006 and then was

20 OpenNet Initiative, “China,” full source link http://....
21 OpenNet Initiative, “Iran,” full source link http://....
sporadically available until 2009 when it was blocked again across the country.

The BBC Persian service has the most page views per month (40 million) of all non-English language BBC websites. BBC Chinese has 9 million page views ranking it as eighth highest. The BBC calculates unique users (UUs) weekly. There are an average of 650 thousand UUs for the Persian service and 152 thousand UUs for Chinese.

Both China and Iran adapt information controls in reaction to breaking news stories and sensitive political events. The ONI describes this agile form of control as just-in-time-blocking—a phenomenon in which access to information is denied exactly at times when the information could have the greatest potential impact, such as elections, protests, or anniversaries of social unrest.22

China has blocked social media websites during lead ups to sensitive events such as the twentieth anniversary of Tiananmen Square and has gone to the extreme of completely severing Internet connectivity in the autonomous region of Xinjiang in response to ethnic riots.23

During the 2009 protests over disputed presidential elections in Iran, government authorities implemented a range of reactive information controls including blocking access to social media platforms used by activists to mobilize protests, and introducing new legislation that prohibited the use of circumvention technologies and distribution of information threatening to the regime. Iranian authorities also engaged in aggressive surveillance of mobile networks and social media platforms to monitor protesters’ activities.24

The restrictive communications environment and legal and regulatory frameworks in China and Iran, coupled with the regimes’ tendency to adapt information controls to sensitive events, makes them challenging markets for delivering news content and suitable test beds for assessing strategies for bypassing censorship to ensure news delivery.

The following sections examine how the BBC introduced and propagated web-proxy services provided by Psiphon, in Iran and China. These case studies draw on aggregated statistics of Psiphon service usage. For security and privacy purposes, Psiphon does not make information available that could identify individual users or IP addresses. However, it can provide daily aggregate statistics showing the following information for each proxy server:

- Number of users logging in
- Country of login
- Number of pages requested
- Host name requested

With the propagation strategies separating the channels for each server (Twitter, email news, broadcast, etc.), it is possible to identify a pattern of usage over time. The case studies analyze the usage data over four specific periods, correlating them with news events and propagation of the nodes.

The data reveal general usage patterns for the proxies since they were first introduced in mid-2009. This analysis also demonstrates what happens when a node is blocked or partially blocked, how it can be detected through usage

---


23 “Chinese Censors Cut off Twitter, Hotmail and Flickr,” The Times, 3 June 2009, full source link http://....

patterns, and the impact blocking has on the introduction of new nodes.

Following this section is analysis of recent events in China and Iran. The China study explores propagation strategies and censorship during the 2011 anniversary of the 1989 Tiananmen Square protests. The Iran study focuses on the 2011 anniversary of the 2009 presidential elections and protests. In each of these cases, we assess the controls that were in place and the strategies used to bypass blocks of the content during sensitive political events.

INTRODUCTION OF BBC WEB-PROXY SERVICES IN IRAN AND CHINA

During the period of the Iranian presidential elections in June 2009 and subsequent protests, the BBC Persian website was suddenly blocked across the country. This was the first blocking episode since the BBC Persian satellite television station was launched several months earlier.

During the block, the BBC observed a significant increase in traffic to the BBC Persian TV Internet live stream, representing more than four times its usual levels. Geographical IP lookups of this traffic showed that the majority of streaming was from inside Iran. In reaction the BBC began to find ways to let the audience know that it could still access the streaming media.

Psiphon provided proxy servers configured with bbcpersian.com as the first page that would be seen after logging in. The BBC used bit.ly, the URL-shortening service, to set up links to Psiphon servers and to the direct-media streams, and used all available channels to promote the availability of BBC content: email newsletters, Twitter, Facebook, and on-air promotions. The use of bit.ly allowed the BBC to look at near real-time statistics showing from which country the shortcut URL was being accessed. A separate web page was created to carry the BBC Persian TV stream through a non-BBC HTML player that was not being blocked in Iran.

Following the introduction of the webproxies during the disputed presidential elections, the service was not as actively promoted, but by mid-2010 was still showing steady usage, with an approximate 5 percent weekly growth rate. During this time the node was propagated through links in email newsletters. This period was a comparatively steady phase for the BBC Persian service, and the growth pattern for use of the Psiphon proxies remained the same from August 2010 through to the Arab Spring events in February 2011.

While the Psiphon service for BBC Persian was launched in the midst of a sudden blocking of the website and grew organically with limited promotion, the web-proxy service for BBC Chinese was introduced as part of the BBC editorial team’s ongoing strategy and had the full involvement of its production team, who were eager to promote its availability. At the end of September 2010, the BBC Chinese service started to publicize Psiphon node URLs with the message “If you are having trouble accessing our site in China, please try [node URL].”

Psiphon set up three nodes with URLs propagated through different channels by the BBC: one through email newsletters; one through the BBC Chinese Twitter account, and one promoted on air and in direct email contact with individuals.

The frequency of propagation differed for each of these channels. A message accompanied every radio broadcast (three times per day, with additional trails featuring the promotion), email newsletters were sent daily, and Tweets were sent on an ad hoc basis.
Figure 4 shows the total number of logins to the web-proxy through the BBC Chinese Psiphon service compared to BBC Persian during the first eight weeks. The active promotion from BBC Chinese helped the service grow rapidly so that the number of logins matched those seen by BBC Persian service’s Psiphon nodes.

**FIGURE 4: TOTAL NUMBER OF WEB-PROXY LOGINS TO BBC CHINESE AND BBC PERSIAN SERVICES**
MEASURING PATTERNS OF WEB-PROXY USE

Estimating the size of audiences that use the web-proxy service to connect to BBC content can be difficult because growth trends are prone to unpredictable changes, due to either increased use of a proxy or a sudden drop in its use.

A web-proxy service can become suddenly unavailable due to direct blocking actions implemented by government authorities or ISPs. Over the period of the BBC trial, there were several occasions where the proxy service was suddenly blocked. Figure 5 shows total logins through one particular BBC Chinese proxy server propagated through radio that was available from February to April 2011. The service was promoted on air, at the end of each hourly bulletin on the BBC Chinese radio service. While there was a generally positive growth pattern for the proxy server, the graph clearly shows its use dropping dramatically on 28 March 2011.

FIGURE 5: TOTAL LOGINS TO BBC CHINESE RADIO WEB-PROXY NODE
The date at which this particular node was stopped is significant. On the previous Friday, 25 March 2011, BBC Chinese radio ended its Mandarin broadcasts, and so there was no channel for the BBC Chinese service to propagate a replacement node. The blocking of this node was therefore particularly effective, and showed that the node may have been allowed to exist in the short term by censor authorities who knew that they would be able to block it on a particular date.

The effectiveness of a block on any service is not always this obvious, and can depend on the willingness of individual ISPs to block content as requested by authorities. Blocking of proxies in China is particularly noticeable due to the uniform implementation of filtering at the backbone level, which makes blocking events appear almost instantaneously across ISPs. However, because infrastructure in other countries is provided through a number of different routes, authorities are unable to block individual URLs across multiple ISPs with the same level of ease or speed.

Figure 6 shows Iranian usage of the BBC Persian social media web-proxy node in January 2010. At a time when the node was reported by some audience members to be blocked, the graph shows an immediate decrease in logins of around 76 percent, but still maintains a daily average of 160 logins. Data on multiple Iranian ISPs were not available, but the usage pattern suggests that a partial block of the node may have been occurring in the country, possibly by one of the major ISPs.
Another main driver for a change in the use of web-proxies can be a news event, in which the broadcaster may see a sudden upturn in use of its circumvention services. Users interested in a breaking story can increase service usage, but increased use can also lead to greater attention from authorities and subsequent blocking of individual nodes.

One measure of success for a proxy deployment can be derived from analyzing the number of requests per login. For the first year from July 2009 to July 2010, the BBC Persian service was experiencing approximately seven to twelve page requests per login session. Within the period between August 2010 and October 2010, this rate increased to average between seventeen and twenty page requests per session, a rate that was maintained through July 2011 (Figure 7). BBC Chinese has also seen a fairly steady number of requests for each login since the service’s introduction in October 2010, with weekly averages of between seven and fifteen requests per session. Note that these requests are for all content, not just BBC pages, suggesting that, as the service matures and attracts a core audience, that audience trusts the service enough to use it as a matter of course for their web browsing.

![Figure 7: BBC Persian Requests per Login (Weekly), July 2009 - July 2011](image-url)
Figure 8 shows the impact of a new node propagated through online radio broadcasts. The blue line shows a node that was propagated via radio broadcasts, and which was blocked at the end of March 2011. The orange line represents a replacement node propagated over online audio broadcasts from the end of May 2011.

When the replacement online audio service started and propagation began, it quickly reached the same level as before. This particular node started to see a sharp increase in requests per login from the beginning of July 2011. This increase is similar to the previous situation with the BBC Persian service’s increased usage, and shows that there is probably a core audience who have absorbed the propagation message and are using the proxy service for regular browsing. There is no significant difference in requests per login for registered users compared with guests.
This data takes into account all sites visited for each login. When looking at BBC sites only, the number of requests per login is far lower. On the BBC Persian site, looking specifically at requests from the target market (Iran or Unknown) from January to July 2011, the average number of BBC pages viewed is 2.2 per session. This number is much lower than the BBC’s reporting of visitors to its sites globally, where the average number of page requests per visit to bbcpersian.com is between 3.4 and 3.8.

For the Chinese proxies, the number of BBC requests per login for China or unknown location is 3.6. This number is significantly higher and exceeds the BBC’s own global average of 3.2 to 3.5 page views per visit to bbczhongwen.com.

The difference between the BBC requests per login for China and Iran can likely be attributed to the difference in audience size. The Iranian nodes have a far higher user base, which correlates with a lower proportion of BBC sites being accessed, as the proxy becomes used more for accessing a range of sites and services, but still with BBC pages as their first stop.

This analysis also suggests that the time taken in building up the Iranian audience on the webproxies has made the BBC trustworthy—Iranian users find that the service the BBC provides is genuine and reliable. If the audience is willing to use the service to access sites other than the host’s, then they are using the nodes as part of their everyday browsing experience, and are willing to trust the provider to enable them to circumvent censorship.

2010 NOBEL PEACE PRIZE CEREMONY

Shortly after the BBC Chinese service started propagating the availability of Psiphon nodes, a news event led to additional blocking of BBC content inside China. The Nobel Peace Prize ceremony to honour Liu Xiaobo was due to take place in Oslo on 10 December 2010. On the morning of 9 December 2010, the BBC published a story with the headline “Nobel: China Blocks Foreign Websites Ahead of Ceremony” which reported on the blocking in China of a number of sites, including Norwegian broadcaster NRK. Blocked BBC websites included the main English news site, and bbcukchina.com, an educational site with content about life and culture in the UK that is not normally blocked. The blocking event also caused an increase in undeliverable email newsletters for BBC Chinese.

The BBC worked with Psiphon to offer two extra proxy servers that would provide login screens in English, and bring visitors directly to the BBC news site in English. The first was promoted via Facebook and email newsletters during the day, while the second node was brought online at night via Twitter promotion. Plans were made to provide a video feed of the live ceremony that would be BBC-branded, but not hosted on a BBC website. A bit.ly URL was created for this feed. Editorial teams were instructed to propagate that message only one hour before the start of the ceremony to minimize the probability of it being discovered and blocked by authorities.

Of the two separate nodes brought online for the BBC news site in English, one was blocked almost immediately, while the other was available throughout the weekend. On the day of the ceremony, there were 387 logins from China to this server. A live stream of the ceremony was also created on a non-BBC-branded page, with bit.ly URLs promoted one hour before the ceremony. While the BBC did
not expect a large audience for this stream, data from bit.ly shows that there were 4,236 clicks to the linking URL that day, with around 50 percent originating from China. This traffic accounted for about one-third of the total visitors to that stream, including those accessing it from unfiltered locations.

On 13 December 2010, the BBC news site in English was available again in China, which was reported by the BBC with the conclusion, “China appears to have done what it could to stop unfiltered news of the event reaching its own people.”

The situation in China at this time led the BBC to examine the proxy servers’ availability in the country when a sensitive news item was breaking. The BBC Chinese news service has been systematically blocked in China since it began, but the English site has been mostly available. Proxy servers intended for China had been available up to the point of the Nobel Peace Prize ceremony, but were then actively blocked over the few days before and after the event.

In the months following this event, the BBC propagated Psiphon nodes again, using a number of different channels. The most successful of these was a node propagated through radio broadcasts, with hourly reminders of how to view the BBC Chinese site. However, at the end of March 2011, the radio broadcasts ended due to cuts in the funding of BBC World Service. Within days, the Psiphon node was blocked, severing the audience the BBC had been building up, since the propagation channel could no longer be used. The blocking of this particular node showed that the Chinese authorities were still monitoring what the BBC was promoting, and ready to block direct content and proxy servers when necessary.

2011 TIANANMEN SQUARE PROTEST ANNIVERSARY

The twenty-second anniversary of the 1989 Tiananmen Square protest and subsequent government crackdown was 4 June 2011. In China information about this event is pervasively censored online and across major media outlets operating in the country. In the lead up to previous anniversaries of the event, the Chinese government has increased censorship of specific content to control possible dissent. For example, in preparation for the 2009 anniversary, reports circulated that the regime had blocked access to popular services including Twitter, Hotmail, Flickr, and MSN spaces. This increased filtering was coupled with the arrests of activists and censorship of local and international media reports on the anniversary. The main BBC English news website focused on this crackdown for several days and discussed issues surrounding Tiananmen Square and the impact it had on the Chinese people. On the anniversary date itself, the BBC reported that police had stopped people from entering the square, and were preventing media outlets from filming in the area. A vigil in Hong Kong that day was attended by an estimated 150,000 people. The BBC English page was not blocked during this period.

For the twenty-first anniversary in 2010, the Chinese authorities blocked Foursquare, the location-based social media platform, reportedly in reaction to users reporting to the site that they were “checking in” to Tiananmen Square as a way of memorializing the anniversary. Reports also emerged about a number of

26 “BBC Website Unblocked in China,” BBC News, 13 December 2010, full source link http://...

27 “China Blocks Twitter, Hotmail, Flickr before Tiananmen Anniversary,” OpenNet Initiative Blog, 2 June 2009, full source link http://...

28 “Hong Kong Holds Tiananmen Vigil,” BBC News, 4 June 2009, full source link http://...
blocked websites becoming accessible again including a number of pornographic websites and the video-sharing site Vimeo. The sudden unblocking of this content led some analysts to speculate that it may have been the product of a configuration error rather than an intentional action. 29

The sensitivity of the anniversary and previous evidence of China targeting censorship around the event led to the hypothesis that there was a high probability the authorities would increase information controls in preparation for the event. In particular, we were interested to see if reporting of the event would lead to blocking of BBC English. Given the past blockages of BBC websites in reaction to the Nobel Peace Prize ceremony, it seemed plausible that the Tiananmen Square anniversary would trigger similar blocking behaviour. To test this hypothesis we actively monitored for blocking events before, during, and after 4 June 2011, using the standard ONI Internet filtering verification methodology. In addition the BBC attempted to build up its Chinese audience of proxy users over the period of the anniversary by propagating nodes through all available channels.

Web-proxy Use Before the Anniversary

In the months leading up to the anniversary, there had been several events that affected the use of the BBC Chinese proxy servers. Following the blocking of nodes in reaction to the Nobel Peace Prize ceremony in December 2010, the BBC Chinese service started to propagate new nodes from mid-January 2011.

The number of total logins to the new nodes exceeded the daily pre-Nobel level logins to the original nodes. This change in usage is correlated with a number of high-profile news stories reported through February 2011, including the Arab Spring protests and Jasmine Revolution protests. Online content related to these events was blocked in China, so it is possible that users interested in reading international press on these issues spiked usage in BBC web-proxy logins.

In addition to major news events, BBC Chinese began to promote one particular node’s availability through their Mandarin radio broadcasts. This node accounted for the largest user base by far, with over 90 percent of all logins. At the end of the growth period between mid-January and the end of March 2011 the BBC stopped the radio broadcasts as a result of budget cuts. Three days later, the proxy node propagated via the radio broadcasts was suddenly blocked (Figure 9). Anyone who had registered as a user on the site was notified via email of a new address to use, but around 95 percent of the logins to the server were unregistered users, all of whom would have been cut off from the proxy service.

The timing of this node’s block meant that it had the most dramatic effect, which was the immediate loss of almost the entire proxy audience for BBC Chinese. The BBC service had no replacement radio broadcast, and so was unable to reach out to its audience with an alternate address. At this time, BBC Chinese began to consider alerting people to the registration process, which involved providing only an email address and a password so that communications could be sent out when a node was blocked.

During April and May 2011, the web-proxy use started to build up again, this time primarily through links in the daily email newsletter. By the beginning of June 2011, the nodes were receiving around two hundred logins per day.

29 “China Blocks Foursquare, Unblocks Porn,” OpenNet Initiative Blog, 4 June 2010, full source link http://....
Propaganda Strategies

Throughout June 2011, in the lead up to the anniversary and afterwards, the BBC Chinese team used four propagation strategies. Each of these methods would use a basic message saying: “If you are having trouble accessing our content, please try [URL].”

- **Twitter** – regular messages, one to three times per week, sent out via the @bbcchinese account. While Twitter was known to be blocked inside China, it was believed that this message was re-propagated widely through other channels and helped to build up an audience in the country.

- **Internet Radio** – As radio broadcasts had ceased at the end of March, a new online bulletin program was being distributed, with links to a web-proxy.

- **Email Newsletter** – Daily email newsletters were sent out, containing links to a proxy server.

- **Direct emails** – If anyone inside China contacted BBC Chinese directly to get help accessing the site, they would be sent a direct link to one particular node, not propagated through any other channel.

Although the message was the same as that used on previous occasions, this time the editorial team was changing the message on Twitter...
depending on the situation. Having received reports from some people of difficulties accessing the URL, they added a line to say that the nodes were operational, and to contact the BBC Chinese service if there were problems. Additionally, the message was changed to encourage people to create an account on the server, saying that this would give them technical support in the event of the node being blocked.

This message was an attempt to persuade proxy users that it was safe for them to register. Trust is one of the key issues when providing circumvention technologies, and it is likely that the trust placed in the BBC Chinese’s editorial proposition would have led their users to trust the suggestion that registering would help BBC provide a continuous service. Following this change in the propagation message, 30 percent of logins to the Twitter node were from registered users, compared with just 14 percent across other propagation methods.

**Observations**

Our hypothesis that the anniversary would trigger increased blocking events did not bear out in the evidence. We conducted daily accessibility tests in China from 28 May to 30 June 2011, with a sample of 2,228 URLs. Within this period 464 URLs were found blocked with little variance between the periods around the event and no evidence of increased filtering beyond typical levels documented by the ONI. In addition there were no secondary reports of increased blocking. BBC Chinese proxy nodes also remained operational, and there were no reports of additional content blocking of BBC services.

One day prior to the 4 June anniversary, on 3 June 2011, the node-promotion message was sent out as normal, but for a whole new suite of nodes. Having expected the currently available nodes to be blocked, this propagation was an attempt to keep the service alive by making all-new URLs live so that any reaction would have to be immediate. This strategy was devised following the Nobel event, where nodes that were brought up late on the Friday were available for the entire weekend before they were blocked. This switching of nodes, combined with a more aggressive propagation strategy, was expected to attract attention from the authorities. However, the service continued to grow over the month, and by the end of June 2011, the number of logins per day had risen to over three hundred, approximately 50 percent more than in May 2011.

A number of usage spikes occurred in July 2011 that were correlated with breaking news stories. For example, early in the month there was a spike in logins to the BBC Chinese proxy service that correlated with news stories on rumours spreading online that former Chinese president Jiang Zemin had died. Chinese authorities attempted to control these stories by blocking references to the rumours on blogs and search engines. As observed with previous spikes in usage, following the news event, usage on the web-proxy service went down to a number that was slightly higher than previous levels. The week after the usage spike the number of logs was approximately 17 percent higher than the week before (Figure 10).

30 “Jiang Zemin Death Rumours Spark China Web Crackdown,” BBC News, 7 July 2011, full source link http://...
The higher level of usage continued until 26 July 2011, when a sudden usage spike and a correlated major news story were observed again. Following a bullet train collision on 24 July 2011, in which dozens of people died, a nationwide rail safety campaign was set up amidst compensation claims and anger from relatives. The train crash itself did not cause a spike in usage of the web-proxy service, but news stories show that coverage of the aftermath was subject to censorship by the Chinese authorities.31 On 28 July 2011, all of the BBC’s promoted web-proxies were blocked, leaving the BBC Chinese service once again having to bring up new proxies and restart the propagation.

Using one node per channel of propagation enables us to analyze how each medium contributed to the growth of the service. It was possible to isolate spikes that were due to particular channel promotion and analyze the growth rates caused by different propagation strategies (Figure 11).

31 “China Struggles to Censor Train Crash Coverage,” BBC News, 28 July 2011, full source link http://...
The different methods of propagation gave the BBC Chinese service an understanding of how to reach the audience for different types of circumstances:

- **Twitter** – Useful for spiking the audience logins; the more a message is retweeted, the more people access the service. However, this method is also responsible for the service being accessed by a higher proportion of people outside of China, who see a message on Twitter, follow the link, and log in just briefly.

- **Internet radio** – As with radio broadcasts, spoken links in Internet bulletins helped to achieve a steady growth rate for the nodes. These nodes experience spikes around news events, suggesting that these nodes reach a core news audience.

- **Email newsletters** – This propagation method seemed to reach a steady audience throughout June 2011, having seen its period of growth mainly in the two months prior. The BBC Chinese service had resumed regular propagation through email newsletters after the end of their radio broadcasts,
and had reached the audience level they had seen when they had previously propagated through this channel.

- **Direct emails** – The use of these nodes is very small, which is to be expected since the existence of the nodes is made known to only a very small audience (those who contact the service directly).

The propagation strategies are vital for building an audience and for establishing trust, as was evident by the increasing number of registered logins. However, it is news events that appear to drive the service forward, creating spikes in proxy use that then lead to a growth in regular usage.

**2009 IRANIAN ELECTION AND PROTESTS**

Around the time of the Iranian presidential elections in June 2009, the BBC Persian website was suddenly blocked in Iran. The site had been blocked on previous occasions, but this was the first blocking event since the BBC Persian satellite television station was launched several months earlier. BBC Persian TV was also blocked, prompting a blog post from the BBC’s director of global news to claim that such actions were “against international treaties on satellite communications.”

During the block, the BBC noticed a significant increase in traffic to the BBC Persian TV Internet live stream of more than four times its usual levels. Geographical IP lookups of this traffic showed that the majority of streaming was from inside Iran. The BBC began to find ways to let the audience know that it could still access the streaming media.

Psiphon proxy servers were configured with bbcpersian.com as the landing page that users would see after logging in to the service. The BBC used bit.ly to set up links to Psiphon servers and to the direct media streams, and used all available channels to promote the availability of BBC content: email newsletters, Twitter, Facebook, and on-air promotions. A separate web page was created to carry the BBC Persian TV stream through a non-BBC HTML player that was not being blocked in Iran.

---

32 “Iran Blocks BBC Persian Website,” BBC News, 24 January 2006, full source link http://....

Figure 12 shows bit.ly usage data from when the proxy servers were first promoted by the BBC Persian service. While the initial peak in activity quickly settled down, the news event helped to establish an audience to the proxy servers, and the majority of users accessing the bit.ly links came from inside Iran.

The peak of activity came from the first day of promotion, when BBC Persian actively linked to the Psiphon nodes through their social media channels, primarily Twitter. Sixty-five percent of the 3,709 people logging in to Psiphon nodes on 17 July 2011 were accessing Psiphon through the URL promoted via Twitter. The message on Twitter was repeated twice during the following week, before propagation stopped. After this point, the use of the social media node very quickly dropped off, and in the second week, the node saw only around a third of the amount of logins. The sharp decline of that node was partly due to the news story becoming lower on the agenda, but it also signalled the start of a pattern that would be repeated many times.

At the end of the year, further unrest in Iran led to another round of promotion for this node. The message was sent out again via Twitter from 24 December 2009, and repeated regularly until mid-July 2010. This propagation caused some large spikes to logins over this node, and repeated repropagation of the node helped to establish an audience that continued to visit the proxy service after this period. While the average number of logins to the social media node
between September and November 2009 was 85 per day, the period from the end of January to March 2010 saw this audience grow to around 320 logins per day.

While these usage statistics were encouraging in terms of building up an audience for the BBC Persian site in Iran, it also showed that the message had to be put out every few days to maintain the momentum. In restrictive environments, finding a balance between ensuring users are aware of web-proxy nodes and keeping a low profile from censors can be difficult because increases in propagation can in turn increase the probability of a node being discovered and blocked. In mid-March, reports from the audience suggested that the social media node had been blocked. Use of alternative proxies at this time suddenly picked up, as registered users were migrated and the lower frequency for promotion of alternative nodes kept them available.

2011 ANNIVERSARY OF 2009 IRANIAN ELECTION AND PROTESTS

The previous case study showed the impact of the BBC introducing Psiphon nodes to its audience inside Iran during the period surrounding the 2009 elections. With the second anniversary of the protests approaching, the BBC had seen a sustained period of growth in use of its proxies, although some recently introduced nodes had been reportedly blocked in the preceding three months.

At the time of the first anniversary, the BBC had three available Psiphon nodes, one specifically for propagation through Twitter, and two “general” nodes that were promoted through the website and broadcast media. Use of these nodes had grown steadily over the first five months of 2010, and regular weekly peaks were in excess of two thousand logins per day. During the second half of August 2010, reports were sent in to the BBC from their website users claiming that the proxies were blocked. Whereas in China this would be immediately apparent, Iranian filtering has been seen to take place over several days, as ISPs obey the mandates they receive. Over the period of three days at the end of August 2010, logins to the BBC-provided proxy servers went from over 2,500 to less than 300. Without any further periods of intense propagation, logins to the nodes remained under 1,000 per day until February 2011, when protests across the Middle East and a renewed availability of the nodes led to the service being used more extensively again.

As we did for the Tiananmen Square anniversary, we hypothesized that the sensitivity of the event and the Iranian regime’s aggressive information controls would likely result in blocking of news sources and possibly BBC web-proxy nodes in reaction to protests on the ground. We utilized the same methodology as in the China case study, analyzing ONI testing data and Psiphon usage statistics to monitor possible censorship activity around the event.

Web-proxy use before the anniversary

Use of the BBC-promoted nodes had been growing steadily since mid-February 2011, when the threat of additional blocking was at its highest. From 1 February 2011, mass demonstrations in Tehran led to two reported deaths and many injuries. There were reports leading up to this period that some Internet services, including circumvention tools, were being throttled.\(^{34}\)

In mid-April 2011, all Psiphon nodes were reported to be blocked. An email sent to the BBC Persian service reported: “It seems the...

---

\(^{34}\) “Tor: Increased Internet Blocking in Iran,” The Internet of Elsewhere, 12 January 2011, full source link http://....
proxy you introduced is not working. I just [want to] know if [it] is under construction or has been blocked by authorities? It’s been a week that connection to the proxy is refused.” This report was a false alarm, because technical problems had brought the service down, and unfortunately went undetected by the BBC.

In the last week of April 2011, as usage was reaching 4,000 logins per day, it was again reported that two nodes were partially blocked, which Psiphon confirmed. Two new web-proxy servers were brought online, both of which experienced blocking within a week. However, apart from a noticeable dip in logins for the days surrounding the blocking event, usage remained high as users migrated successfully to the new nodes.

Additional propagation effort in mid-May 2011, particularly through social-networking channels Twitter and Facebook, saw usage of the nodes exceed 5,000 logins per day. The propagation also coincided with news events—14 May 2011 marked the third anniversary of Iran’s jailing of seven Baha’i religious community leaders, and on the same day an Iranian man sentenced to being blinded as a punishment for throwing acid in woman’s face had his sentence postponed (Figure 13).35

Just before the end of May 2011, the node propagated through email newsletters was blocked. Registered users were migrated to a private backup node, and a new publicly promoted node was created.

Propagation Strategies

Propagation strategies utilized in Iran were very similar to those adopted for China in June 2011.

There were three nodes promoted:

1. **Broadcast** – Links to a proxy server were mentioned in bulletins, on BBC Persian radio and television channels.

2. **Email newsletter** – Daily newsletters sent out by the BBC Persian team, with links to the web proxy.

3. **Social media** – One node was used on both Facebook and Twitter, as the potential audience inside Iran for both of these sites was particularly low, due to the number of followers of the BBC Persian service.

Additionally, two nodes categorized as “general” were available for use. These nodes had previously been reported as being partially blocked, but were still serving an audience that accounted for 15 percent of the total logins in May 2011. These nodes are not promoted by the BBC Persian service, but are known to an existing audience, and have remained unblocked for eighteen months.

Blocking events over the previous two months had led to the number of logins at the end of May 2011 being around 1,700 per day, compared to the recent peak of just over 5,000 on 16 May 2011. While this number was still higher than had been observed for much of the year to date, it was still far below the levels the service was expected to reach, and there was a concern that consistent blocking of the nodes could prevent the service from growing.

35 “Iran Acid Blinding Punishment Postponed,” BBC News, 14 May 2011, full source link http://....
CASTING A WIDER NET: Lessons Learned in Delivering BBC Content on the Censored Internet

FIGURE 13: PERSIAN NODES FEBRUARY-MAY 2011

2011

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 Feb</td>
<td>Iran protests — <a href="http://www.bbc.co.uk/news/world-middle-east-12447225">http://www.bbc.co.uk/news/world-middle-east-12447225</a></td>
<td></td>
</tr>
</tbody>
</table>
| 19 & 20 Feb| Iran protests — http://www.bbc.co.uk/news/world-middle-east-12513479
http://www.bbc.co.uk/news/world-middle-east-12519418                                   |                                                                      |
| 21 Feb     | Expected reduction following news stories                                               |                                                                      |
| 26 Feb     | Iran nuclear plans — http://www.bbc.co.uk/news/world-middle-east-12588621                |                                                                      |
| 12 March   | Iran to compete in Olympics — http://www.bbc.co.uk/news/uk-12724166                      |                                                                      |
| 28 March   | Partial blocking of email node                                                          |                                                                      |
| 7 April    | Email node unavailable for several days                                                 |                                                                      |
| 11 April   | Email node available again                                                              |                                                                      |
| 28 April   | Iranian men sew lips in protest at failed asylum bid
http://www.bbc.co.uk/news/uk-england-london-13214907                                   |                                                                      |
| 30 April   | Ahmadinejad “boycotts” work http://www.bbc.co.uk/news/world-middle-east-13250309        |                                                                      |
| 6 May      | Social media node blocked                                                                |                                                                      |
| 14 May     | Acid blinding / Fears for jailed leaders (already referenced)                           |                                                                      |
| 19 May     | Social media node blocked                                                                |                                                                      |
| 29 May     | Email news node blocked (started on 26 May)                                             |                                                                      |
Observations

Similar to the Tiananmen Square anniversary findings, our hypothesis of increased blocking of events was not confirmed by the data collected. We conducted daily accessibility tests in Iran from 10 to 30 June 2011, with a sample of 1,711 URLs. Within this period 618 URLs were found blocked with little variance between the periods around the event and no evidence of increased filtering beyond typical levels documented by the ONI in the country. In addition, there were no secondary reports of increased blocking.

Despite the attention that the BBC’s nodes had received from the Iranian authorities leading up to June 2011, no blocking events were witnessed during the month of the anniversary. Instead, the service as a whole grew steadily, ending the month with a weekly peak of just under 4,000 logins per day. This rate is higher than had been seen in the three months leading up to June 2011, excluding days with major news breaking.

The overall usage of the service was lower than in May 2011, which was largely due to a nine-day period in May 2011 where timely tweets surrounding major news events caused logins through the social nodes to grow to around eight times higher than days surrounding them. In June 2011, social media logins remained relatively flat at approximately 125 logins per day, with a peak on 1 June 2011, when the replacement node was brought online.

Most of the growth in the service was due to the success of the replacement node brought online for propagating through email newsletters. Previous email nodes had experienced a high level of use in the preceding months, but were not growing significantly. In June 2011, the service grew by 70 percent, ending the month with a usage level approximately 50 percent higher than the node it replaced.

One way to assess the growth in use of the nodes is to compare propagation methods to the general nodes. Because the general nodes are not promoted, they tend to have a fairly constant usage pattern. While logins may increase during breaking news events, the assumption is that the same core audience is using the service more frequently.

The general nodes also have the most pronounced weekly cycle, with Fridays being the low point in usage, as illustrated below over a three-month period. This is similar to normal patterns of web use in Iran, where Friday is the last day of the weekend. The dates on web-proxy usage graphs are in Eastern Standard Time, so there is also a relatively low use seen on Thursday, due to the eight-hour time difference.

Figure 14 shows how the growth patterns for different propagation methods varied from the growth in logins to the general nodes.
**CASTING A WIDER NET: Lessons Learned in Delivering BBC Content on the Censored Internet**

**FIGURE 14: PERSIAN NODES JUNE / JULY 2011**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 June</td>
<td>New email nodes brought online, social nodes propagated.</td>
<td></td>
</tr>
<tr>
<td>15 June</td>
<td>Growth peak for social node through propagation.</td>
<td></td>
</tr>
<tr>
<td>8 July</td>
<td>Email news node blocked.</td>
<td></td>
</tr>
<tr>
<td>17 / 18 July</td>
<td>July 17 was a religious holiday in Iran, and therefore usage was low; on the following day an increase was expected, but may be higher due to increased conflict between Kurdish insurgents and the Iranian government.</td>
<td><a href="http://www.bbc.co.uk/news/world-middle-east-14189313">http://www.bbc.co.uk/news/world-middle-east-14189313</a></td>
</tr>
<tr>
<td>30 July</td>
<td>Total usage exceeds pre-blocking levels, illustrating the two-week period that it takes to restore the service.</td>
<td></td>
</tr>
</tbody>
</table>
Following the anniversary period, the node promoted through email newsletters was again reported as blocked on 8 July 2011. As with other blocking events in Iran, the service did not drop off completely and immediately but instead took place over eight days. This gradual blockage is due to how the Iranian authorities filter sites, as ISPs take on board the instructions they are given. While total logins to the service were decreasing, a new node was brought online and promoted again through the email newsletter. This node grew in use over its first two weeks and by the end of the month was performing comparatively with the previous node (Figure 15).

**Figure 15: Persian Email Nodes June / July 2011**
The break in service for the email node shows that the blocking event has an effect on the service that lasts for approximately two weeks before the number of logins reaches previous levels. This break demonstrates that once a node is unavailable, only part of the audience will switch over straight away to the new nodes. Relating back to the BBC / SecDev report on the use of proxies in Iran, this observation illustrates the importance of trust and reliability in providing a circumvention service.

Despite the break in service and the effect on logins to the available nodes, the overall use of proxy servers continued to grow in July 2011, with an increase in logins of just over 7 percent. As with the Chinese study in the same month, the use of individual channels for propagation showed how the service was growing. However, the usage pattern in Iran was very different. While China’s spikes were driven by tweets, propagation, and news events, the Iranian users of the BBC’s proxy servers followed a fairly generic weekly cycle of workday peaks and low usage at weekends.

There was a perceived risk to the service during June 2011, but as the month passed, there were no additional blocking events beyond those experienced at the end of May 2011. Instead, a general growth pattern for the service was seen, mostly due to the success of the node promoted through email newsletters. Throughout the month of June 2011, logins to other propagated nodes remained fairly static.

With email newsletters driving up the traffic, there is also a belief that a regular audience exists through the general nodes. It is normal in Iran for services to be “partly blocked,” as ISPs in the country restrict services in different ways. By keeping the general nodes alive and un-promoted, it is possible to keep a regular audience that is already using the nodes, with less fear of a sudden blocking.

**PROPAGATION STRATEGIES ACROSS THE CASE STUDIES**

The BBC’s experience of propagating web-proxies in China and Iran demonstrates that different propagation channels have different strengths. The different characteristics of each channel and how they can be utilized in news media delivery strategies are outlined below.

**Audio broadcasts**

Radio and TV broadcasts across the BBC regularly promote BBC websites. Both BBC Chinese and BBC Persian have regularly promoted Psiphon nodes over the air, which has helped to build an audience for both services.

From January to March 2011, BBC Chinese regularly promoted a node over their Mandarin radio broadcasts. The node URL was numerical, making it easy to remember and not likely to be misspelled. The audience for this node grew steadily over the three months in which it was promoted until access was cut off on 27 March 2011, shortly after the radio broadcasts were stopped.

Following the cessation of Mandarin radio broadcasts, BBC Chinese began to provide online audio programming, and Psiphon nodes are regularly promoted during these broadcasts. The audience for this node has also started to see some growth, and now accounts for approximately 33 percent of the total number of logins to the proxy servers.

**Email newsletters**

Disseminating web-proxy URLs through email newsletters can be a very effective way of steadily building an audience over time. Both BBC...
Chinese and BBC Persian regularly add links within their regular email newsletters, so the link will always be at hand for anyone receiving the email, whether directly or forwarded.

There have been occasions where, particularly for BBC Chinese, large quantities of emails suddenly bounce back to the sender. However, emails are still believed to be regularly passed around between people both inside and outside of the target country.

Figure 16 shows two “phases” of propagation using email newsletters for BBC Persian. The node was reported as being blocked on 29 May 2011, at which point the use dropped off almost completely. A new node was brought online the following day, and reached a usage level similar to the previous node within a week. During June 2011, use of this node continued to grow steadily, due to being constantly promoted in the email newsletter at a time of heightened risk in the country.
Twitter

From the very start of the BBC’s efforts to propagate nodes for BBC Persian in Iran, the dramatic effect of tweeting a message was clear. Figure 17 shows two periods of activity, the very first tweets in July 2009, and then further tweets amid unrest in Iran at the very end of the same year. Use of the nodes dramatically lowers after the period of tweeting is complete.

FIGURE 17: ACTIVITY ON BBC PERSIAN NODES JULY 2009-MARCH 2010
This particular node was also linked in email newsletters, so some of the growth that was experienced can be attributed to that channel. However, examples also exist of nodes being propagated exclusively through Twitter.

During the period surrounding the Tiananmen Square anniversary in June 2011, the BBC Chinese service regularly promoted their Psiphon node using Twitter. The result was an initial flurry of additional logins, but rather than settling back down completely, there was a return to around double the previous usage level. The repeated propagation, two to three times per week, helped to start building up an audience for the service. Messages were also retweeted by other users of Twitter, and although the number of retweets was minimal, they presumably helped reach people who were not accessing the BBC Chinese twitter feed directly.

Full-text RSS feeds

The BBC Persian website is publicly available as a full-text RSS feed. This feed can be an effective way of getting content into Iran, since individual blogs and other news providers can put the content into their own site. As an example, blog.malakut.org regularly pulls in feeds from BBC Persian, and iPhone apps have been created for both BBC Persian and BBC Chinese, with a private developer making use of RSS feeds to deliver the content into the target market. RSS feeds can also deliver content directly to the audience. China Digital Times’ newsletter (http://chinadigitaltimes.net/) has carried content pulled from BBC Chinese’s RSS feed for delivery into China.

Two main challenges exist for broadcasters who make this content available through RSS feeds. First, it can be difficult to control who reproduces the content, and in what context. The BBC makes most of its content available over RSS to its formal business partners only and public RSS is limited to headline and summary text. However, these business-to-business partnerships are not possible in restricted markets, so if the content is to be carried externally it needs to be publicly available in the first place.

The second challenge is in measuring the reach of content carried over RSS. While a broadcaster will be able to see how many times its feeds have been accessed, there is a disconnect when the feeds are ingested into another site, and the broadcaster will not necessarily be able to track where its news then appears.

URL shorteners

For many of the propagation strategies explored by the BBC, URL-shortening services such as bit.ly are used to send URLs that are easy to remember, or URLs that are obscure and less likely to be targeted for blocking. The main advantage of using a URL-shortening service is that it gives access to near-real-time statistics, which means that the broadcaster can see instantly how many people are clicking the link, and (in the case of bit.ly) the geographic location of users. This capability enables richer assessment of social media propagation because the broadcaster can measure how sustainable its message is and how often it is being repropagated by users.

More importantly, URL shorteners can help to provide early notification of content blocks. In the case studies for BBC Persian and BBC Chinese, the majority of visitors to the bit.ly URLs were from the target countries. If the broadcaster is monitoring the stats from bit.ly, it can monitor significant decreases in the number of clicks to its site and changes in geographic location, which can help to verify blocking reports.
from the web audience.

This method of detection works only if the blocked URL is the shortened version. However, there have been cases confirmed where the shortened URL is still available but the node itself is blocked. The assumption is that the people or processes responsible for blocking URLs are seeing only the final URL that is accessed. The first time this was seen by the BBC was for a BBC Persian proxy server propagated mainly through Twitter. The node itself was available from January 2010 but was blocked in mid-March 2010, but no replacement was propagated until August 2010. Access to the bit.ly stats interface shows that the audience carried on trying to access the link until the new one became available.

The theory that only the final URL is blocked also applies to China. Accessing bbczhongwen.com through testing agents shows that the initial .com domain is available, but that the connection is reset after it redirects to bbc.co.uk. This pattern also applies to proxy servers that are propagated using short URLs—the shortened URL remains available while the proxy is blocked.

During the period of the 2010 Nobel Peace Prize, one Psiphon node that was brought online the day before had a discrepancy between the number of people accessing the bit.ly URL and the number accessing the node. This difference helped in establishing that the node was immediately blocked, so a new one could be prepared.

These findings suggest that the difference between bit.ly and Psiphon statistics can show when a node is blocked and possibly indicate technical problems with a node. In the following example, a technical outage for a node in August 2010 was accompanied by a surge in attempts to access it through bit.ly. So although the bit.ly URL was working correctly, the URL for the node was unavailable.

It is normal to see the underlying URL blocked, with bit.ly clicks still active. However, there is also evidence showing times when only the shortened URL appears blocked, and not the node itself. Following the period of technical outage in August 2010, bit.ly links to BBC Persian’s Psiphon servers were reported as being blocked in Iran. While there was a reduction in the number of people accessing nodes due to their bit.ly links being unavailable, this was the first time that the bit.ly clicks were lower than logins to the node. This showed that the bit.ly links had been blocked, at least by some ISPs, but that the nodes were still available and still being accessed.
CASE STUDY TAKEAWAYS

Blocking events are unpredictable and require agile reaction from broadcasters

Despite the aggressive filtering tactics of China and Iran and previous increases in information controls during the events and anniversaries we monitored in the case studies, we were surprised that we did not find increases in general filtering or blocking of BBC nodes. Blocking events can be unpredictable and while broadcasters may prepare for events that seem likely to meet greater information restrictions, the level of censorship may not change as expected. Interestingly, we also found that controversial breaking news stories were correlated with increased blocking of related content and increases in web-proxy usage, which suggests that authorities may increase restrictions in reaction to sudden events that broadcasters are not able to predict.

The dynamic and unpredictable nature of censorship requires broadcasters to be agile in their circumvention strategies. In reacting to blocks, it is possible to experience only a minor break in service, as long as replacement nodes are available and quickly propagated. Trust is important; broadcasters need to make sure the service they offer is both technically reliable and always accessible to an audience that is reaching out for news and information.

Real-time blocking detection is essential

To react in a timely and effective manner to blocking events, news broadcasters require as close to real-time detection of blockages of services as possible. There are different blocking methods depending on the country, so any real-time alerts need to be verified, but in each case there will be sudden drop-offs for traffic to websites or proxy servers. By reacting quickly to these blocks, the broadcaster will minimize the time in which its service is unavailable.

Propagation strategies should be diversified

Each method of propagating a circumvention service can be considered a “channel” for distribution. The URL promoted on air should be different than that sent via email newsletters, which in turn should be different from the URL promoted via a social-media channel such as Twitter.

Each method of propagation has its own strength

Different methods of web-proxy propagation have particular strengths. Twitter is useful for short-term boosts in usage, but will also increase the number of logins from outside the target country. Email newsletters and promotion over traditional broadcast media did not result in the same level of usage peaks but helped steadily grow audiences. Direct communications with links to private nodes can be effective for reaching a core audience that trusts the service.
5. ALTERNATIVES TO PROVIDING CIRCUMVENTION SERVICES

When considering how to help its audience bypass censorship of its content, a broadcaster can do more for technical delivery of its content than providing circumvention tools. Broadcasters can work to ensure content is delivered through web-proxies and other circumvention tools, make use of CDNs and distribution strategies that push content through multiple domains, and also push content out in formats that allow it to be ingested through other sites and applications. These strategies expand on early attempts to bypass censorship by mirroring content. For example, Deutsche Welle experimented with creating a mirror of their Chinese news offer so that it could reach an audience in China. This site was successful in reaching people inside China, and lasted for approximately a year before it was blocked.

LIMITATIONS OF DELIVERING CONTENT THROUGH WEB-PROXIES

Delivering news media through web proxies can have limitations that may impair the user experience. For example, due to known issues with Psiphon v2, BBC sites are not always rendered correctly through the service. Freedom House noted this issue in their review of circumvention software, pointing out that web-based proxies have an “inability to properly translate flash and some other forms of dynamic content.”

There are two areas of concern for the BBC pages:

1. Page structure: There is a heavy reliance on JavaScript, particularly on the index pages of language news sites such as bbcpersian.com. Content is fully displayed with correct links, but the editorial placement of news stories can be obscured by incorrectly rendered JavaScript modules.

2. Audio and video: Audio and video on the BBC’s language websites is served using Flash Player or Windows Media Player, which will not be accessible through a web-proxy.

To address these issues the BBC could work with Psiphon to improve content caching and JavaScript delivery. This approach has proven to be successful with Voice of America sites, which render properly using Psiphon. However, many modules on the BBC language news sites are used to render sites covering all of the BBC’s entertainment output as well as its news. Changes made in this environment to support serving content through web proxies would likely be considered low priority. An alternative is to consider changes that will have an effect on only the language news sites, such as modifying the CSS.

Audio and video on the BBC’s language web sites play using Flash Player or Windows Media Player. This content will not be playable through a web-proxy. The embedded video on news pages is encoded as a 392kbps Flash video, and played over RTMP. Links to alternative Windows Media versions (225kbps and 34kbps) play through the Windows Media MMS protocol.

While the BBC-embedded media player will remain as Flash for the time being, the underlying video itself does not have to be Flash.
encoded. The BBC is producing some audio and video content in formats that can be delivered via HTTP rather than RTMP. This standards-based approach allows content to be consumed on newer mobile devices, specifically those with support for HTML5, and will make BBC content more accessible through Psiphon and other web-proxy tools. BBC sites with audio and video available over HTTP have been successfully tested over Psiphon.

USE OF CONTENT DELIVERY NETWORKS

The BBC’s international news services have distributed audio and video content through Akamai since 2003, and URLs for the streaming media do not include bbc.co.uk. Instead, Akamai’s edge network handles the stream request so that the server providing content to the end user is the one nearest to that computer on the network.37 Because the servers are not specific to the BBC, URL and IP-based blocking becomes more difficult than targeting *.bbc.co.uk. There have been reports of individual machines on Akamai’s network being blocked, which has led to “thousands of websites” also being made unavailable.38 The effects of such filtering are much wider than the blocking of an individual site.

BBC streaming media are also available over other CDNs. iPhone streams, using HTTP-chunked data, are provided by StreamUK, as are MP3 audio streams over SHOUTcast. Again, the obscurity of the URL means that they are less likely to be blocked. Statistics related to these streams show China in the top-ten list of countries receiving these streams. The audience in Iran counts for less than 1 percent of the audience for these streams.

Live streams are available to mobile devices through non-BBC URLs such as iPhone video streams and SHOUTcast MP3 streams, while news clips for mobile devices are provided in discrete indices on the mobile version of the website, with device detection and media hosting through a CDN. Clips are available through HTTP, so web-proxy users can consume BBC language news videos through the mobile sites. However, the video index is provided as only a chronological list and offers no editorial content ordering.

The final hosting place for streaming media is for clips aimed at mobile devices, and is provided by YoSpace. Their platform receives RSS feeds from the BBC, converts videos, and handles device detection so that the appropriate video format is played. When this service was introduced to the language news sites, it was shown in discrete indices from the mobile version of the website (e.g., bbcpersian.com/mobile/video), with the videos themselves played through an appropriate YoSpace CDN server. The video index also makes clips available to non-mobile devices through HTTP, so the mobile video index is one way in which web-proxy users can consume BBC language news videos. However, the video index is again provided as a chronological list only, without editorial content ordering.

RSS AND SYNDICATION

The BBC’s language news content is created using a Content Management System that was written in house. As well as making sure the content all fits into the defined template for news stories, this makes it possible for the news stories to be written once, and then get customized

37 “Streaming,” Akamai, full source link http://....
for different platforms. The content management system writes content formatted for:

- BBC websites (e.g., bbcpersian.com)
- BBC mobile sites (e.g., bbcpersian.com/mobile)
- Syndication platforms

For most BBC language news sites, only headline and summary text is available for public syndication, with full-text offers restricted to commercial deals. However, for BBC Persian, there is a “full-text” feed available publicly because the BBC recognizes the difficulty of serving content into Iran. This format, and its availability in multiple blogs and websites, makes it difficult for Iranian authorities to find and block BBC content.

RSS feeds are also used to distribute content via iPhone apps that have been created by an enthusiast of the BBC Persian site. The developer uses the RSS feeds to recreate web content inside the app, and also links to the live audio and TV streams, and on-demand video files, carrying web content over HTTPS. The Chinese application is available in China’s app store—information from the developer suggests that downloads inside China count for over 50 percent of the total for the app.

Where only headline and summary text is published to the website as an ATOM RSS feed, there is still a full-text version created. This is made available to partners for B2B syndication, and is often transformed into different formats of RSS, depending on partner requirements. Most content provided in this way comes through commercial deals with third parties, where contractual arrangements are in place to govern how the content is carried and branded.

Syndicating content in this way may cause problems for the partners because they would have to retrieve the RSS feed, transform it, and host it on their own site. This will make them more susceptible to being blocked themselves. For the BBC Chinese news site, there are no partners inside China that will carry the content, but for the BBC UK China educational site, syndication deals usually account for 95 percent of the site’s traffic. There are no reports of partners suddenly refusing to carry BBC content from bbcukchina.com, but anecdotal evidence suggests that some content is rejected due to government directives sent to the partner banning certain terms.

The BBC Persian site, which carries only news content, has no formal B2B syndication deals for text and images. The only commercial deal is via gooya.com, which carries a link back to the BBC site for all content and the site does not receive the BBC news feeds.

Audio and video content is also syndicated; one of the BBC’s partners for its language video content is YouTube. YouTube channels exist for BBC Persian and BBC Chinese, as well as several other BBC languages. Statistics from YouTube show that when YouTube itself is available, BBC videos can be viewed through the site inside both Iran and China.

By recognizing the need to provide content through multiple channels and services, a broadcaster can begin to deliver its content in a way that makes it far more difficult for censors to block. The broadcaster must acknowledge that there is more to bypassing censorship than merely providing circumvention software, and instead needs to adapt its delivery strategies to maximize the chance of its content getting through to its target audience. The wider the pool of URLs, and the wider the content delivery strategy, the more difficult it becomes to restrict the flow of information.
6. SUMMARY AND RECOMMENDATIONS

It takes a thorough understanding of the distribution environment for Internet content for a broadcaster to bypass censorship of their content online. This report shows that bypassing censorship takes far more than the provision of circumvention tools, and requires investment in, and careful management of, a clear strategy. To reach an audience that otherwise has no access to the broadcaster’s content, the strategy has to be adaptable and allow for unexpected events. The following recommendations will help the broadcaster to formulate a strategy that will both make its services available to an audience, and help it to grow an audience using circumvention tools.

Be clear about objectives

Broadcasters need to clearly define what they hope to gain from providing Internet censorship-circumvention services. The objective of the circumvention strategy we outlined here was to deliver content to audiences in countries where filtering is pervasive and BBC content is blocked. However, the delivering of content to such environments does not necessarily require only circumvention software. Broadcasters may also benefit from combining circumvention technologies with adaptive content that can be carried through other websites and media channels.

Circumvention technology can be useful for delivering content to an audience that cannot access a broadcaster’s content, but based on the experience of the BBC studies these tools are usually effective for disseminating content to only a relatively small, but interested audience. In countries where content is pervasively blocked a large portion of the potential audience may be unaware of the existence of the broadcaster’s circumvention service. Attempts to grow the BBC audience in China showed that the web-proxies were reaching a small audience, but audience feedback sent directly to the BBC Chinese service suggests that the proxies were being accessed by users who were interested in news content and grateful for the accessibility.

New delivery platforms require commitment and investment

Reaching audiences in restricted environments through circumvention technology represents a new kind of news-delivery platform that requires infrastructure, investment, and strategic thinking from broadcasting organizations. If a broadcaster decides to provide circumvention services to enable access to its content, it needs to ensure the software meets the needs of its target audience and is accessible, secure, and scalable.

Once the technical infrastructure of a circumvention service is established, broadcasters require an ongoing investment to manage it to ensure performance and effective and dynamic propagation that can be adjusted to address changing circumstances. The ongoing management of a circumvention service requires understanding current restricted markets, and trends in markets that may come under threat of content filtering and other restrictive Internet controls. To gain this understanding the broadcaster will need to research the communications ecosystems of these markets or outsource such research to experts in the field.
These requirements mean that investment in this new delivery platform needs to be ongoing and will increase the overall distribution costs associated with Internet content delivery. Circumvention tools tend to have a higher cost-per-user associated with them than delivery of content over the open Internet because of the additional costs for managing what is effectively a bespoke delivery platform.

There are political connotations of “circumvention” that makes the distribution of content through these tools more of a strategic challenge for broadcasters who may be reluctant to be involved in the wider debate around censorship and freedom of expression on the Internet. Therefore, the circumvention tools a broadcaster chooses need to be considered part of the general distribution strategy for news content, and not as a completely separate activity. Propagating the nodes and referring to them as another content-delivery platform will de-politicize the message being sent out.

**Be adaptive**

Internet censorship is dynamic and can vary significantly between countries and regions. Broadcasters need to adapt to different environments and be able to implement strategies that address shifting requirements and challenges. Effective delivery strategies must consider technical variance in filtering, the political climate that enforces censorship regimes, and the social nuances of the audience the broadcaster is trying to reach.

Strategies for propagation of circumvention tools will also need to be agile. The case studies in this report show how different methods of propagation can be used in different circumstances, both for immediate impact and the long-term growth of a proxy service. Depending on the news agenda, the broadcaster may be able to use multiple propagation methods to maximize its reach through circumvention software. Editorial teams will therefore need to work closely with technical and market experts to know when and how to propagate different ways to access content.

Knowledge of a country’s technical infrastructure will help in deciding which methods to use when bypassing censorship. For example, the BBC and the SecDev Group’s research in Iran showed that due to the high cost of accessing the Internet, many Iranians are unable to afford high-speed access. Under such restrictions broadcasters must adapt their content in ways that can be consumed by narrowband audiences.

Syndication of content may also be crucial for getting content into restrictive environments. Allowing multiple third-party websites to carry news stories may make content blocking more difficult if content will be spread across a number of different URLs. While many syndication deals can be business-to-business, the content will be more widely syndicated if it is available to individual blogs and small websites. However, this option makes the measurement of audience reach more difficult for the broadcaster, so it will have to adapt its measurement strategies to allow for content distributed in this way. This is a decision that needs to be made at the strategic level, weighing the importance of measurement against the need to make content available to the audience.

**Collaborate with stakeholders**

Individual broadcasters will need to devise their own strategies for bypassing censorship and propagating circumvention software that meet their organizational objectives. For example, the BBG may be distributing software with a clear agenda to provide access to a free and
open Internet, whereas the BBC is currently trying to reach and grow an audience for its own content only. However, the two organizations, along with other similar broadcasters, are facing common hurdles in delivering their content. By working together and regularly addressing the issue of content delivery in restricted markets, news broadcasters will be able to increase their understanding of the restrictions placed on them, and use common approaches where appropriate.

In terms of detecting censorship and being able to understand when content is being blocked and when it needs to be addressed, broadcasters have access to server logs and other analytical services that show the flow of data across their audience in many countries. This data could be combined with information from other organizations and content-delivery networks that also have their own systems. While much of this data would be commercially sensitive, aggregated information and analysis, such as that seen in Google’s Transparency Report, could be shared between broadcasters and other companies who are providing services over the Internet, to present a global picture of Internet censorship’s impact.

Additionally, broadcasters should work closely with other stakeholders. Broadcasters can bring their own in-depth knowledge of the broadcasting environment to academics who are studying Internet censorship, and other organizations who are trying to deliver content into restricted markets. By sharing information for research and public education, it will be possible to increase the understanding of the problems companies and individuals face in distributing information and participating freely in discussions using the Internet.
7. AREAS FOR FURTHER RESEARCH

Due to the accessibility of data from the corporation, this report focuses its analysis on the BBC’s experiences with web-proxies. While examination of this data has been sufficient for an initial look into the challenges that confront international broadcasters delivering content online, a wider study across multiple organizations would help to develop and test further hypotheses.

The following areas of research would help to both extend broadcasters’ understanding of the problems they face in distributing their content into restricted environments, and to make them better prepared in dealing with the changing nature of Internet censorship.

**Real-time Internet censorship detection**

This study has shown that international broadcasters require near real-time detection of service blockages to react in a timely and effective manner to censorship of their online content. GeoStats provides a proof of concept for one possible approach to this challenge. Further research and development is required to build a system that can meet this requirement. Work should also be done on systems and methods for correlating data on broadcasting service blockages with other Internet censorship data available from research projects like the ONI, Herdict, and industry efforts such as the Google Transparency Report.

**Comparative study of international broadcasters**

This study is limited to a single broadcaster. Having access to multiple broadcasters’ data would enable not only a comparison between broadcasters, but also a more detailed study of the correlation between news events and increased proxy usage. Additionally, with the BBC being relatively new entrants in the field, adoption of their proxy servers is still relatively small, particularly compared to BBG. Combining data sets and utilizing a combination of statistical and qualitative analyses will help move toward further understanding the impact of news events and blocking events on the different services.

Beyond other broadcasters, there should also be further study in a wider set of countries. China and Iran were chosen for the prevalence of blocking and data availability. Other countries and information-control regimes present different challenges for broadcasters that require comparative study.

**Suitability of other circumvention software**

This report concentrates on web-proxy servers, and considers the BBC’s perspective that web-proxies are the most suitable circumvention tools to propagate for its circumstances. Further research could analyze other software’s potential for distribution by broadcasters. This work could include assessing the benefits of software that allowed full multimedia access against the support burden and political connotations of distributing software intended to circumvent legal restrictions.

**Commercial news provision**

Many commercial broadcasters also provide international services, whether through traditional broadcast platforms, newspapers, or Internet services. How can they meet the
challenges that are detailed in this report, and does it make commercial sense for them to try and reach audiences in countries where their content is either blocked now, or could be at any point? This line of inquiry would also consider the possibility of providing commercial circumvention tools, examining how a sustainable commercial model could be introduced to help audiences consume unrestricted access to the Internet.

The challenge for mobile delivery

Internet access on mobile devices is a growing opportunity for content providers, but is also proving to be subject to its own set of content controls, varying widely between countries and telecom providers. Broadcasters are delivering more news content to mobile devices than ever before, and delivery to these platforms forms a core part of any news strategy. Research is required to assess what broadcasters need to do to ensure their audience can continue to reach their news output in these increasingly restricted environments.

Collaborative multistakeholder frameworks

One of the key recommendations from this report is the value of multistakeholder collaboration. Further research could help to formulate a framework under which this collaboration could operate, highlighting areas where different organizations would benefit from sharing their data and experiences. It could also help to evaluate different technologies and approaches from the perspective of news delivery and audience reach, to complement other research into tools for general Internet access and for activism.
8. SUGGESTED READINGS


