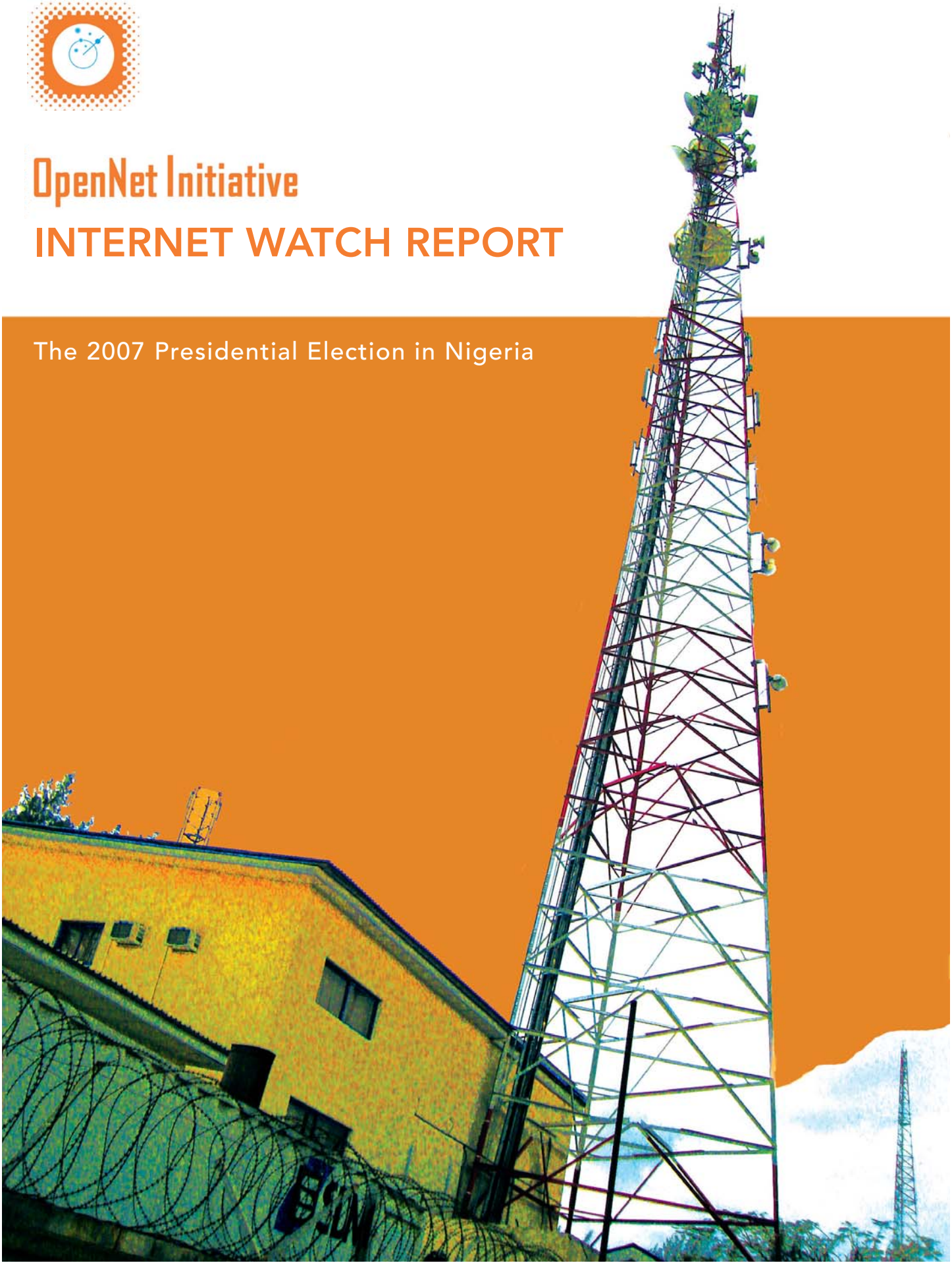
OpenNet Initiative

INTERNET WATCH REPORT

The 2007 Presidential Election in Nigeria



About the OpenNet Initiative's Internet Watch Reports

Internet Watch Reports document emerging trends in Internet filtering and control. These occasional reports take a detailed look at events, policies, technologies and countries where filtering and content controls are occurring in new and unexpected ways, or where filtering has been alleged but undetected using conventional ONI testing methodologies. They are designed to test hypotheses, refine monitoring techniques, and report on the global informational battle space. Internet Watch Reports are available for download at http://opennet.net.

About the OpenNet Initiative

The OpenNet Initiative is a partnership between the Advanced Network Research Group at the University of Cambridge, the Citizen Lab at the Munk Centre for International Studies at the University of Toronto, the Berkman Center for Internet & Society at Harvard Law School, and the Oxford Internet Institute at the University of Oxford. Work on this Internet Watch Report was supported through a grant from the John D. and Catherine T. MacArthur Foundation, which also supports ONI as a whole. For more information about the OpenNet Initiative, please visit ONI's Web site, http://opennet.net.

Acknowledgments

The research presented in this report could not have been completed without the time and effort of the ONI team, as well as our team of infield researchers based in Lagos. 'Gbenga Sesan, a member of the field team, was responsible for much of the background research of the political, legal and telecommunications environment in Nigeria that informs this report. Along with 'Gbenga, the other members of the field team—Mary Joyce and Ugo Nwosu, an unpaid volunteer—worked on the logistics of the project, which turned out to be more of a challenge than anticipated. ONI's election testing methodology and design specifications for the dedicated testing device were developed by Rafal Rohozinski (Advanced Research Network Group, University of Cambridge). Steven Murdoch (ARNG, Cambridge) programmed the dedicated testing device and was very active in troubleshooting with the field team. Nart Villeneuve and James Tay (Citizen Lab, University of Toronto) assisted the field team in the configuration of the primary testing program and also analyzed results. The research effort was coordinated by Rob Faris (Berkman Center for Internet & Society, Harvard Law School). The report was written by Mary Joyce. Sally Walkerman (Berkman Center, Harvard) and Jane Gowan (Citizen Lab, Toronto) contributed to editing, layout and production of this publication. Finally, thanks to Ronald Deibert (Citizen Lab, Toronto), John Palfrey (Berkman Center, Harvard), and Jonathan Zittrain (Oxford Internet Institute) for their editorial and substantive input to this report. ONI is solely responsible for any errors or omissions in this report.

Contents

Executive Summary

Despite widespread charges of fraud and disenfranchisement, Nigeria's recent elections were not marked by Internet tampering. While certain sensitive political sites were inaccessible around the time of the elections, these blockages were not caused by intentional tampering but rather by structural problems in Nigeria's faulty telecommunications network. The results of the technical monitoring included no evidence of attempts to block or disable Web sites critical of the current regime, either during or directly preceding the elections. These conclusions were reached through the analysis of tests carried out by the OpenNet Initiative, a partnership between research institutes at the universities of Cambridge, Toronto, Harvard, and Oxford.

The ONI team conducted two types of tests during the election period, which were carried out by a field team in Lagos and researchers in Cambridge, UK. The first testing program, developed by ONI researchers, was run from a standard personal computer. Researchers on the ground in Nigeria used the program to attempt to make contact with a list of politically sensitive sites using several Internet service providers (ISPs) and then sent the results of those tests back to the Citizen Lab at the University of Toronto for analysis.

The second series of tests were run through a specialized computer designed to interact with networks, which was controlled remotely by technical researchers at the University of Cambridge. Testing began a week before the local elections and continued through the national elections. The ONI has been developing technical methods of monitoring for evidence of just-in-time Internet filtering or other tampering with Internet access during election periods.

The ONI has conducted Internet-related election monitoring in Kyrgyzstan and Belarus prior to these tests in Nigeria. The ONI ran the election monitoring project in Nigeria because of widespread concerns that the elections would not be free and fair. Observers have claimed that both the local elections of April 14, as well as the national elections on April 21, were marred by blatant and widespread violence, fraud, and disenfranchisement. In reference to the elections on April 14, Peter Takirambudde, Africa Director of Human Rights Watch, stated that “the Nigerian government failed completely in its conduct of a free and fair election” in several key states. Commenting on the presidential elections from the northern town of Kaduna, Max van den Berg, head of the European Union's Observer Mission, noted, “for now the assessment is outspokenly negative ... I'm very concerned.” In addition, the National Democratic Institute went so far as to say that the elections represent “a step backward in the conduct of elections in Nigeria.” Nevertheless, the elections appear to have been free from Internet-related attacks and Web site blocking.

Introduction

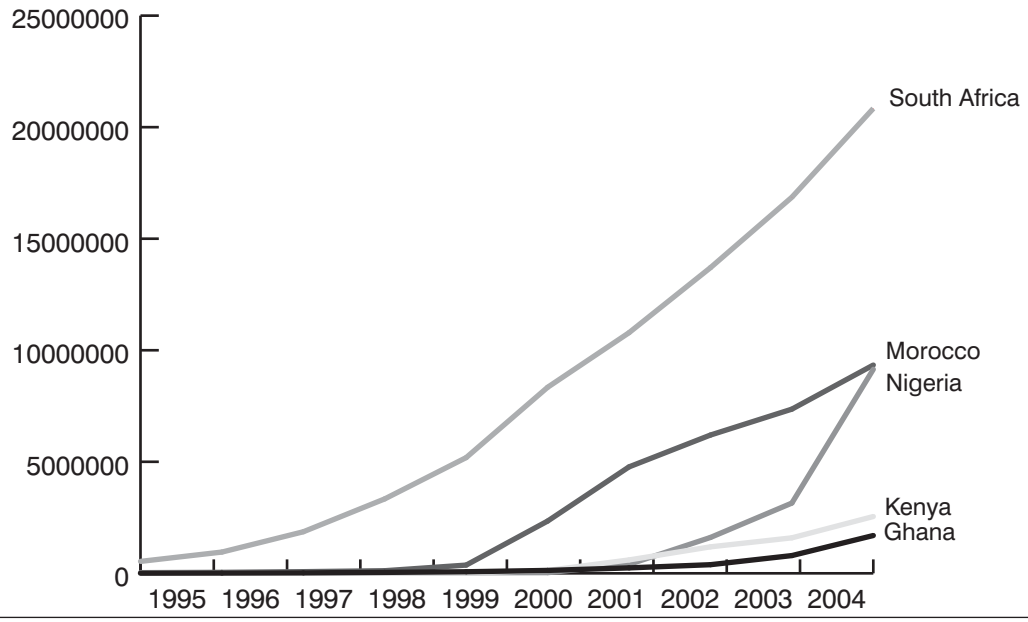
The Nigerian Context

Africa's progress towards stable democratic systems of government since the end of the colonial era has been slow. According to one measure championed by the US-based nongovernmental organization (NGO) Freedom House, in 1976 just three countries in Africa were said to be "free," while twenty-five were "not free." Thirty years later, the number of "free" countries has grown to seven while those deemed "not free" has dropped to eighteen.[1] In addition, all but five countries on the continent have held elections within the last five years (though of varying degrees of legitimacy).[2]

Africa has also been slow to enter the digital age, and lags significantly behind other regions of the world in this respect. That said, the past decade has seen a narrowing of the digital divide. Cell phone ownership has risen exponentially in many African countries, with wireless lines often outnumbering land lines. Similarly, access to the Internet is also rising, albeit at a slower pace due to the limitations imposed by forces such as high levels of poverty, illiteracy and lack of basic infrastructure.

The graphs below show this growth for five representative African countries. Although the two graphs have similar growth patterns, note that the final totals are quite different. The highest national figure for cell phones is 20.9 million subscribers, while the highest figure for Internet is only 3.5 million users, both in South Africa.

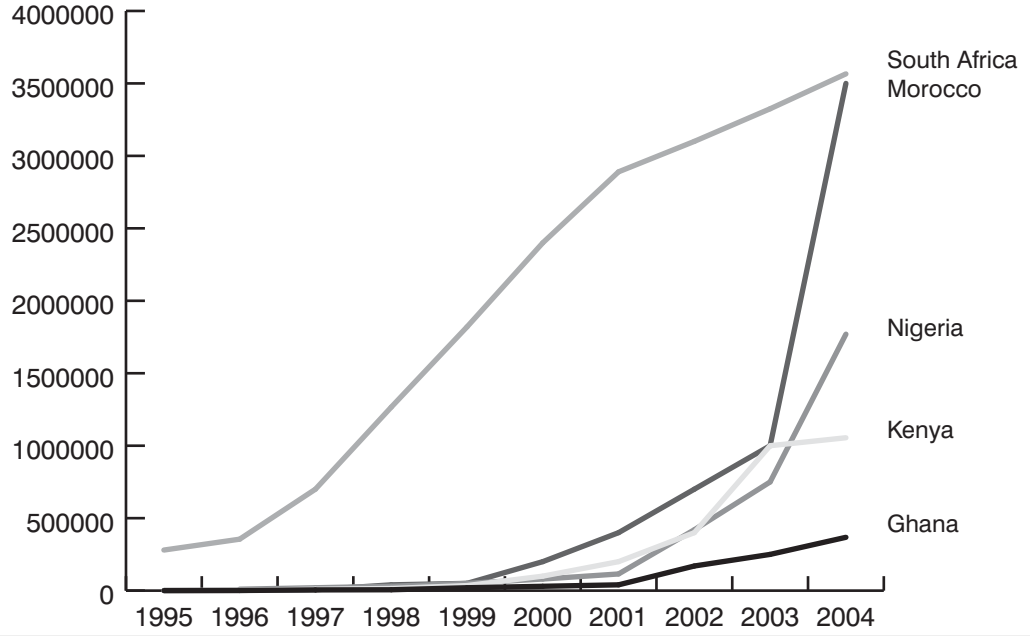
Graph 1. Growth of Cellular Phone Subscription in Africa (1995-2004)
Source: The International Telecommunication Union (complete figures in Appendix)



[1] Lydia Polgreen, "Africa's Crisis of Democracy," The New York Times, 23 April 2007, online edition (www.nytimes.com); Map of Freedom 2006 at www.freedomhouse.org

[2] The countries which have not recently held elections are Angola, Cote d'Ivoire, Eritrea, Libya, and Somalia. In this context, "recent" means within the last five years.

Graph 2: Growth of Internet Users in Africa (1995-2004 estimates)
Source: The International Telecommunication Union (complete figures in Appendix)



Nigeria is good example of trends in telecommunications development in Africa. Nigeria has experienced one of the most dramatic increases in cell phone ownership of any country in the world, jumping from 13,000 subscribers in 1995 to over 9 million in 2004. In the same period the number of Internet users grew from under 10,000 to 1.7 million.[3] Strong growth has continued; the number of Internet users in Nigeria in December 2006 and January 2007 were 32,322,202 and 33,603,761 respectively.[4]

Nigeria is also an example of a country progressing towards democratic governance. In 1999 and 2003 the country experienced its first and second presidential elections since the end of military rule, and there is great hope that the age of coups and military dictatorships is firmly in the past.

The intersection of technological and political change in countries such as Nigeria is of interest to ONI researchers. While the Internet offers easier access to information and new means of personal expression, it poses a challenge to traditional political interests, and makes it possible for state authorities to implement new forms of political information control and censorship.

Monitoring the Internet during Elections: the ONI Experience

ONI has shown through its past research that countries that do not filter Internet content on a regular basis may nonetheless control Internet communications during election periods, and may use methods subtler than outright filtering or blocking. For this reason, ONI has begun to undertake investigations of the Internet during elections, with Nigeria as the fourth such effort.

[3] International Telecommunication Union Yearbook of Statistics: Telecommunication Services Chronological Time Series 1995-2004, (Geneva, Switzerland: ITU, 2006), 126.

[4] Nigeria Communications Commission subscriber data 2001-Jan. 2007, www.ncc.gov.ng/subscriberdata.htm.

ONI began its monitoring of the Internet during elections with the 2004 US Presidential elections. Testing showed that while President Bush's official Web site was blocked to Internet users outside the country, users within the United States were able to access the site.[5]

ONI election monitoring efforts followed with a larger research project in Kyrgyzstan during the 2005 elections. ONI researchers were able to track two Denial-of-Service (DoS)[6] attacks on ISPs hosting opposition newspapers back to a group of Ukrainian hackers-for-hire. However, ONI was unable to connect this group to the Kyrgyz government. Both the government and the opposition newspapers were able to spin the Web site malfunctions to their own advantage.[7]

In 2006, ONI mounted a third election monitoring project, in Belarus. This project encountered similar challenges to the Kyrgyz project. Several opposition Web sites were inaccessible via the state-owned Beltelecom ISP both on and directly after election day. However, ONI was unable to conclusively prove that DoS attacks had taken place because researchers did not have access to server logs. The fact that these sites were blocked on a network controlled by the regime indicates that official manipulation was the likely explanation. However, ONI found no conclusive evidence of systematic and comprehensive interference by state authorities or their agents with the Internet in Belarus, although it was clear that tampering did occur. The report recommended that election monitoring become a special focus of ONI attention, and that the issue of Internet openness during elections should be raised as an important emerging issue among those groups mandated with measuring the freedom and fairness of elections.[8]

Structure of this Report

In this Internet Watch, we report on ONI's efforts to monitor the April 2007 presidential election in Nigeria. This report is presented in four parts.

Part 1 details why Nigeria was a leading candidate for ONI election monitoring. Nigeria has a long history of electoral manipulation, as well as state control and manipulation of the media. Recently, the government of President Obasanjo initiated legislative and institutional changes to increase the government's ability to control the Internet, with the ostensible goal of curbing cybercrime. In addition, Nigeria's position as Africa's most populous and second-richest country, combined with its active foreign

---

[5] OpenNet Initiative, "Geolocation filtering: www.georgewbush.com blocked during run-up to election," (OpenNet Initiative Bulletin 007, October 27, 2004), http://opennet.net/bulletins/007/.

[6] In a Denial-of-Service (DoS) attack a hacker or group of hackers, usually with the help of automated "bots," make multiple simultaneous requests to a Web site they wish to disable. The goal of the attack is to overwhelm the server on which the Web site is hosted so that it can no longer respond to all the page requests and displays an error message when legitimate Internet users try to access the site. This can be a preferred method of Internet censorship because it is difficult to prove that the Web site is inaccessible as a result of a DoS attack rather than because of an overwhelming number of hits by legitimate users.

[7] OpenNet Initiative, "Election Monitoring in Kyrgyzstan," (OpenNet Initiative Special Report, February 2005), http://opennet.net/special/kg/.

[8] OpenNet Initiative, "The Internet and Elections: The 2006 Presidential Election in Belarus (and its implications)," (OpenNet Initiative Internet Watch Report, April 2006), http://www.opennetinitiative.net/studies/belarus/ONI_Belarus_Country_Study.pdf.

policy, make it an important standard-bearer for African reform—or stagnation.

Part 2 reports on the testing process and findings of the 2007 ONI monitoring carried out during the national and state elections. The testing found no evidence of blockage or interference. While there were several instances where politically sensitive Web sites were unavailable, ONI found that these failures were caused by flaws in Nigeria's weak telecommunications infrastructure rather than deliberate meddling.

Part 3 builds out on the findings and considers a prognosis for Internet freedom in Nigeria. The government's tradition of muzzling dissent along with the new Internet policy environment that is unfriendly towards Internet freedom combine to make filtering seem a possible next step. On the positive side, Nigeria's extremely decentralized telecommunications infrastructure makes the Internet much more difficult to control than in other countries, as the Nigerian Internet does not have fixed 'choke points' through which outside content could be blocked or filtered.

Part 4 provides a short summary of the overall findings of ONI testing in Nigeria.

Part 1. Why Test in Nigeria?

The ONI considered Nigeria an important test case for monitoring the Internet during elections for four reasons: 1) a history of electoral manipulation; 2) the critical nature of the election as the nation's first transfer of power between civilian governments; 3) Nigeria's importance as a bellwether of reform for Africa; and 4) the government's growing interest in regulating the Internet, with the stated goal of curbing cybercrime.

A History of Electoral Manipulation

Following the death of Nigeria's military dictator Sani Abacha in 1998, his successor, General Abdusalami Abubakar, began the process of returning the country to democratic governance. Abubakar set up the Independent National Electoral Commission (INEC) to conduct elections for local and national positions and legalized political parties, which had been forbidden under Abacha. Several new political parties were created, of which the All People's Party (APP), Alliance for Democracy (AD), and People's Democratic Party (PDP) were the most prominent. INEC successfully organized elections in late 1998 and early 1999. Olusegun Obasanjo, a former military leader who had been imprisoned by Abacha, was elected president; his party PDP continues to hold power to this day. Although there were instances of ballot falsification and ballot box stuffing, especially in the perennially troubled Niger Delta oil region, the theme for the day was hope and progress as Nigeria moved out from under the weight of thirty-three years of military rule.

In 2003, Obasanjo ran successfully for re-election, though in this second outing the press and international observers were decidedly more critical of the election proceedings. The National Democratic Institute (NDI) witnessed "vandalised, stolen

The Nigerian Elections in the Blogosphere

Nigeria's bloggers are overwhelmingly affluent and urban, and are thus hardly a representative population. Nevertheless, they offer important first-hand accounts of the election. These bloggers, acting as citizen journalists, noted a salient point overlooked by the mainstream media: while many voters were eager to participate in the democratic process, voter apathy was a considerable problem. Ore of "Ore's Notes" described her experience voting in the local elections on April 14, 2007. "I chided myself for not getting there earlier, but I heard from people who had been there at 8AM, as instructed, that the INEC [election commission] officials had not yet arrived at that time. Thank goodness the line moved (albeit very slowly) and there were interesting conversations going on around me to participate in and listen to."[1] Funmi of "Funmi Iyanda's Blog" had a similar experience on the 14th. "I … stood in line in the sun for two hours, hat and sunglasses firmly on, large bottle of water in hand as resolutely determined as most of my fellow countrymen to cast my vote," she wrote.[2] However, during the presidential elections a week later, her experience was quite different. "This weekend, the polling booth was a ghost town, my people had lost hope. I voted and left.... I had observed proceeding from the Alimosho area [of Lagos], through Agege, Ikeja, to Maryland and the apathy was palpable. The streets were empty as boys took to the highway playing football."[3] Since many voter tallies were falsified, the actual rates of voter turn-out were often not recorded.[4] Blogger accounts offer important qualitative evidence of true participation rates.

[1] Ore's Notes, "Voting in Progress," April 14, 2007, http://orenotes.blogspot.com/2007_04_01_archive.html.

[2] Funmi Iyanda's Blog, "Power from the People," April 23, 2007, http://fiyanda.blogspot.com/2007_04_01_archive.html.

[3] Ibid.

[4] Ben Rawlence and Chris Albin-Lackey, "Briefing: Nigeria's 2007 general elections: Democracy in retreat," 106 African Affairs 497.

and stuffed ballot boxes"[9] while the leader of the European Union observer delegation, Max van den Berg, said that he was "very concerned" about the voting (he was to repeat the same phrase during the 2007 election).[10] In addition, Human Rights Watch issued a report which argued that at least one hundred people had been killed as a result of political violence.[11]

It appeared that, after only four years in power, the PDP was consolidating their influence, leading one BBC journalist to title his analysis of the 2003 elections "Nigeria's One-Party Creep." In 2005, Obasanjo began an unsuccessful attempt to do away with the Constitution's term limit clause which prevented him from seeking a third term. After failing in this effort, he turned his sights on assuring the 2007 victory of his chosen successor and PDP presidential candidate, Umaru Yar'Adua, the governor of Katsina State.

Obasanjo and the PDP used the courts to keep hundreds of opposition candidates off the ballot, including Atiku Abubakar, the Vice President and Obasanjo's former ally (Abubakar's candidacy was later reinstated by the Supreme Court). In the words of The Economist, "the lengths to which Mr. Obasanjo's ruling People's Democratic Party (PDP) has gone to cling to power have undermined and discredited so many of Nigeria's institutions and office-holders that the country now seems more a prisoner of its bleak past than a beacon for the future."[12] The nation's vast oil riches (valued in 2005 at USD 50 billion per year), combined with limited checks on the executive branch and minimal accountability in the use of public funds, makes Nigeria a tempting prize for any political party. Given these circumstances, the PDP, not surprisingly, seemed unwilling to cede power.

Gubernatorial candidate Jimi Agbaje (right)

Hopes for a Legitimate Transfer of Power

This 2007 election was to be historic, the first time in the nation's forty-seven year history since independence that power would pass from one ruler to another based upon the results of an election rather at the barrel of a gun. While the election of 1999 left many with hope for Nigeria's future, it was not a contest between an incumbent and a challenger, but rather a contest to decide Abacha's successor. The election in

[9] Joseph Winters, "Analysis: Nigeria's One-Party Creep" BBC News, 21 April 2003, http://news.bbc.co.uk/2/hi/africa/2964759.stm

[10] Ibid.

[11] Nigeria's 2003 Elections: The Unacknowledged Violence (Human Rights Watch, 2004), 1.

[12] "How to Steal Yet Another Election" The Economist, April 21, 2007, Vol. 383 Issue 8525, p51-52, 2p, 1c (Hereafter referred to as "How to Steal").

Obasanjo Hot and Cold

The outgoing president, Matthew Olusegun Aremu Obasanjo, is a contradictory figure. His admirers note that he is Nigeria's first democratically elected leader since the 1960's. He also wears the badge of a dissident; he was imprisoned by the military dictator Sani Abacha for criticizing his regime. In addition, Obasanjo has a reputation as a corruption fighter. His economic reforms inspired the Paris Club to forgive $18 billion of Nigeria's debt in 2006[1] and he has served on the advisory council of Transparency International. Yet recent actions have seriously damaged his reputation. In 2005 he pushed the National Assembly to alter the constitution to allow him to run for a third term,[2] allegedly offering bribes to lawmakers willing to support him.[3] Once this effort failed, he set about the task of ensuring that power passed to a member of his own party. According to the Economist magazine, "Mr. Obasanjo has pursued a highly partisan campaign by manipulating and abusing the very institutions, such as the elections commission and the anti-corruption agency... that were touted as paragons of his reforms, so undermining their hard-won credibility in the eyes of many Nigerians."[4] We now doubt whether history will look fondly upon Obasanjo or his political legacy.

[1] "Nigeria settles Paris Club debt," BBC News, April 21 2006, http://news.bbc.co.uk/2/hi/business/4926966.stm.

[2] Toye Olori, "Uproar over Obasanjo's third term campaign," News from Africa (December 2, 2005), http://www.newsfromafrica.org/newsfromafrica/articles/art_10550.html.

[3] Craig Timberg, "Nigerian Senate Blocks Bid for 3rd Presidential Term," Washington Post (May 17, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/05/16/AR2006051600705.html.

[4] "How to Steal," The Economist.

2003 was also an inconclusive test of the health of Nigeria's democracy. Even in established democracies like the United States, incumbent candidates regularly have an advantage over challengers when running for re-election because they can marshal some of the powers of the state behind their campaigns.[13] Obasanjo's re-election in 2003 did not conclusively point to a dysfunctional electoral system as the president's electoral success could be attributed simply to incumbent advantage.

It was for this reason that the 2007 election was so important. It was a measure of whether Nigeria was really on the path to a stable democratic system of government or, as many feared, elections were being used to legitimize a strongman political system in which he who has the oil makes the rules.

With Repercussions Beyond Nigeria's Borders

Why does Nigeria's political situation matter? In many ways, Nigeria is a bellwether for reform in Africa. It is the continent's most populous country; remarkably, one in five Africans is Nigerian. Its vast oil wealth also makes it Africa's second richest nation after South Africa. In fact, Nigeria's GDP makes up a mammoth 55% of the economic output of the West African region. The United States alone imports more than 1 million barrels of crude oil from Nigeria every day and has pegged part of its strategy of reduced dependence on Middle Eastern oil to imports from Africa.[14]

Nigeria's most significant international influence is in Africa. It helped found the Organization for African Unity (now the African Union) in 1963 and President Obasanjo served as the organization's chairman from 2004 to 2005. Nigeria contributed significant numbers of troops and financial resources to regional

[13] Some of these advantages that US elected officials hold are laid out in "Why are Sitting Members of Congress Almost Always Re-elected?" Citizens for U.S. Direct Initiatives, 2003, http://www.cusdi.org/reelection.htm. The authors analyze some of the numbers at play in the 1998 mid-term Congressional elections.

[14] Jad Mouawad, "Growing Unrest Posing a Threat to Nigerian Oil" The New York Times, April, 21 2007, online edition (www.nytimes.com).

and UN-sanctioned peacekeeping forces that intervened in Liberia's civil conflict in the 1990s. "When there are crises, the countries have looked upon Nigeria to be an arbitrator," said Ngozi Okonjo-Iweala, Nigeria's former Minister of Finance and Foreign Affairs.[15] Nigeria has the economic power, regional influence, and visibility to mark a path to improved governance on the continent—or to excuse other smaller countries from backsliding into dictatorship and political inertia.

A New Internet Policy

In addition to the political situation, the country's changing relationship to the Internet made this election a significant one to monitor. In 2004, the Nigerian Cybercrime Working Group was established by President Obasanjo. The group is charged with "the responsibility to create a legal and institutional framework for securing computer systems and networks in Nigeria and protecting critical information infrastructures in the country."[16]

In 2005, the "Computer Security and Critical Information Infrastructure Protection Bill" was introduced into the National Assembly. The bill is concerned with cybercrimes such as hacking and identity theft, and provides law enforcement with the power to collect digital evidence.[17] If passed, it would make unlawful many undesirable Internet activities, such as spamming, data forgery, computer fraud, cyber-terrorism, and unlawful interception, and it would require that ISPs keep records of all traffic and subscriber information for a period of time to be determined by the president.[18] While it has received a good deal of attention, the Bill appears to be stuck in Assembly and has not yet been voted on.[19]

Defaced campaign posters on an overpass in Lagos

Even though the Bill is focused on providing measures for combating cybercrime, it leaves open the possibility of abuse. At the time of the Bill's introduction, local press noted several provisions in the Bill that appear overbroad, in comparison to similar Bills in other jurisdictions. "[T]here are no checks and balances provisions

[15] "Regional Giant Nigeria Looms over West Africa" The Online Newshour, April 5, 2007, online edition, http://www.pbs.org.

[16] Nigerian Cybercrime Working Group homepage (http://www.cybercrime.gov.ng).

[17] Computer Security and Critical Information Infrastructure Protection Bill 2005, http://www.cybercrime.gov.ng/site/index.php?option=com_content&task=view&id=20&Itemid=56

[18] Ibid., § 11.

[19] Supra note 16.

whatsoever in the Bill. There are no mandatory reporting procedures to either the Nigerian parliament or the Nigerian judiciary on the activities of law enforcement agencies in carrying out these wiretapping or lawful interception activities."[20] There appears to be no recourse for individuals whose civil liberties are compromised. In addition, it was noted that there is, "in the matter of obtaining a warrant [f]or release of information for legitimate reasons, a recurring reference to either a Court of Law or 'any other lawful authority' for obtaining either the warrant or the information. There is no enumeration or definition anywhere in the Bill, as has been done in other jurisdictions, of whom or what constitutes 'lawful authority.'"[21] A number of other worries have been listed, including concern over the security of personal data storage and transmission at ISPs; the ability of the president to make additional regulations pertaining to provisions in the Bill; and a provision that allows for data to be released without a warrant in extreme circumstances without an accompanying provision that requires a warrant to be sought with similar urgency.[22]

In 2007, the Directorate for Cybersecurity (DfC) was founded to "respond to security issues associated with growing usage of Internet and other information and communication technologies (ICTs) in the country."[23] In its first year of existence the new agency was given a hefty budget of USD 9.3 million to accomplish its goal.

These recent actions demonstrate that the Nigerian government would like to control online activities more effectively within the country. While there have been no allegations of Internet blocking within Nigeria so far, the elections served as an excellent opportunity to test Internet freedom there.

Within the Context of Limited Freedom of Expression

These threats to Internet speech arise within a national environment of limited freedom of expression. By one measure, the US government-backed NGO Freedom House currently classifies Nigeria as "partly free" (an electoral, but not liberal, democracy) and gives it a freedom rating of 4 out of 7, where 1 represents the most open societies and 7 the least.

Some newspapers in Nigeria have been controlled by political interests. Two governors, Orji Uzo Kalu and James Ibori, whose terms expired with the spring 2007 elections, are reported to own newspapers The Sun and The Daily Independent, respectively.[24] They both now face charges related to corruption while in office, and Orji Uzo Kalu has fallen out with his former party, PDP.[25] The Guardian, which is widely considered to be an open and objective newspaper and is one of the country's most widespread papers, is

[20] Eijeagbon Ohicheoya, "Nigeria: New Wire Tapping, Cyber Crimes Bill in Nigeria," This Day (Lagos), Oct. 18, 2006, available at http://www.infosecnews.org/hypermail/0610/12262/html.

[21] Ibid.

[22] Ibid.

[23] Shina Badaru, "FG Okays N1.2b for Cybersecurity Directorate" This Day (Lagos), April 6, 2007, available on allAfrica, http://allafrica.com.

[24] Interview, in-country researcher with Mary Joyce, OpenNet Initiative, April 2007.

[25] Email from Dan Smith, Brown University, to Sally Walkerman, OpenNet Initiative, Oct 10, 2007.

also owned by the Ibru family,[26] who are also close to Obasanjo.[27]

In addition, journalists who write about the misdoings of politicians have been harshly punished. In 2005, Owei Kobina Sikpi, publisher of the Weekly Star, was secretly detained for nearly a week and then charged with seven counts of false information after his newspaper published an article alleging that a state governor was involved in money laundering.[28] That same year, members of the State Security Service (SSS) raided the offices of the Lagos-based weekly The Exclusive and confiscated more than 200 copies of the tabloid in an effort to censor coverage of ethnic Igbo nationalist groups.[29] Given the level of corruption in Nigeria, however, it is noteworthy that there is a certain level of press freedom. There are a number of smaller newspapers not owned by politicians, and many print articles that include negative speech about the government.

Because many Nigerians do not or cannot read, radio is an important source of information.[30] In a positive 2005 development, the Nigerian Broadcasting Commission (NBC) decided to auction broadcast network licenses to private operators. (Radio had previously been the unique domain of the government.) This change in the radio market primarily benefited large broadcasting companies. At the same time, the NBC opened a path for community broadcasting licenses for nonprofit stations run by members of a particular locality, though the license regime for community broadcasting is largely considered prohibitive. Despite these recent moves towards greater openness, the Nigerian government maintains control over what is broadcast by refusing or rescinding licenses. The vulnerable position of regime critics makes the Internet a likely next frontier for political control.

[26] Supra note 24.

[27] Supra note 24.

[28] "Nigeria," Freedom in the World (Freedom House, 2006).

[29] Ibid.

[30] As of 2004, literacy was estimated at 68% ("Nigeria," The World Factbook, CIA, http://www.umsl.edu/services/govdocs/wofact2004/geos/ni.html). Radio, especially call-in or SMS-in radio, has increasingly been a mechanism for information exchange in Africa (Ethan Zuckerman, "What is Citizen Media," Panel Presentation, September 21, 2007). NGO Global Knowledge Partnership has found that radio is a good method of communication for locals implementing development projects (See "Virtual Consultations: Build on Local Resources", http://www.globalknowledge.org/gkps_portal/index.cfm?menuid=184&parentid=78).

Part 2. Monitoring the Internet During the Nigerian Elections

ONI monitored the Nigerian Internet for two weeks, beginning a week before the April 14, 2007 local elections and ending two days after the April 21, 2007 presidential elections. No filtering of Internet content, deliberate or accidental, was detected by ONI research.

Methodology: How we tested

Much of the testing took place from within Nigeria. ONI employed two methods to monitor the status of the Nigerian Internet and accessibility of Web sites. First, a field team based in Lagos employed an effective ONI tool to test a comprehensive list of potentially vulnerable Nigerian Web sites. These included political and independent media sites, as well as other sites critical of government or key Nigerian officials. Tests were carried out across five different Nigerian Internet service providers (see Table 1). Test results were then cross-checked against results of the same test run from ONI's control locations outside of Nigeria to determine whether failed connections were due to internal blocking, which would result in an error message only in Nigeria, or a problem originating at the Web site itself (or more general failures in the Internet), which would result in an error message occurring regardless of location.

Second, the ONI field team deployed a dedicated testing machine designed to measure the status of the Nigerian Internet throughout the testing period, recording local network failures and anomalies. This machine was controlled remotely by operators at the University of Cambridge, providing a platform for ONI researchers to perform testing metrics designed to eliminate technical failure as a possible cause of the inaccessibility of websites.

How we chose which ISPs to monitor

In selecting which ISPs to test the team was guided by three criteria: 1) likelihood of being filtered, 2) infrastructural diversity, and 3) availability of dial-up service.

According to the first criterion, Nitel was the most significant ISP to monitor. It is the historic national operator and was owned by the Nigerian government until it was privatized in 2006.[31] Despite being under new ownership, Nitel operates as if it were still government-owned. (The field team had to submit passport-sized photos in order to sign up for an account, making the process feel more like a visa application than buying Internet service.) In addition, one ONI field researcher recalled that a director at Nitel's main facility in Lagos asked the field team to write a letter to Abuja to request permission to place ONI equipment in the building, despite the fact that the Nigerian government should technically no longer have any control over Nitel.

[31] The current owner of Nitel is the Nigerian investment company Transcorp.

Table 1: ISPs Tested

Name	Type of Internet gateway
Hyperia	Highway Africa satellite (Nairobi)
Linkserve	SAT-3 submarine fiber-optic cable (Lagos)
Cyberspace	SAT-3 submarine fiber-optic cable (Lagos)
Nitel	SAT-3 submarine fiber-optic cable (Lagos)
Tara	SAT-3 submarine fiber-optic cable (Lagos)

The second criterion dictated that ONI test a variety of Internet gateways. Because all the Web sites on the test list were hosted outside of Nigeria, it was important to test the integrity of a variety of different paths to the external Internet. There are several reasons why ONI only tested sites located outside of Nigeria. In testing for election-oriented filtering, ONI wished to test opposition sites, which are usually hosted outside of Nigeria. For Africa in general, few sites are hosted on the continent; they are more often hosted by services in other parts of the world.[32] Filtering is also more likely to be found on sites hosted outside the country, as filtering is one of the only ways that a group can limit access to a rival's Web site if it is located elsewhere (rather than simply pulling the plug on servers located in-country).

In Nigeria, the most common types of Internet connection are VSAT (very small aperture terminal) and fiber-optic cable. VSAT is a satellite connection designed for easy deployment which uses a satellite dish of less than 3 meters in diameter. Most large businesses, particularly banks, use VSAT for their Internet connection because it allows them to bypass Nigeria's inadequate telecommunications infrastructure. These businesses use their VSAT dishes to connect to privately-owned telecommunications satellites which route their Internet traffic. The VSAT-based ISP we used, Hyperia, accesses the Internet through a satellite owned by Highway Africa, a news agency based in Nairobi, Kenya.

The second common way to connect to the external Internet is by fiber-optic cable. There is only one fiber-optic cable that connects to Nigeria, the SAT-3/WASC (South Atlantic 3/West Africa Submarine Cable). SAT-3, as it is called, runs from South Africa to Portugal and makes landfall in nine countries along Africa's west coast. SAT-3 is controlled by a closed consortium of historical telecommunications companies, one for each country it connects to.[33] Nitel is the consortium member in Nigeria, and as such controls all Nigerian access to the SAT-3 cable. Other ISPs who wish to use SAT-3 to connect their clients to the Internet must pay Nitel for the privilege.

Monopoly over the SAT-3 cable gives Nitel an excellent opportunity to filter the Internet traffic that passes through that gateway. For this reason, ONI decided to test not only Nitel, but also three ISPs that rent bandwidth from Nitel: Linkserve, Cyberspace, and Tara.

---

[32] Infrastructure, security, and ease of set-up are factors that Web site owners consider when determining where to host a site. For a general discussion, see Ronald Deibert et. al., eds., Access Denied (forthcoming 2008). Regarding security, hosting a site outside the country can help a Web site owner maintain anonymity. See Ethan Zuckerman, "How to Blog Anonymously," Handbook for Bloggers and Cyber-dissidents, Reporters Without Borders, Sep. 2005, http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf.

[33] This arrangement, which gives every consortium member monopoly rights to the cable in their country, is very worrying to advocates of an open telecommunications market.

What we found

There were several sites that were inaccessible at varying times during the testing period, among them the sites belonging to the BBC, Amnesty International, the Human Rights Library at the University of Minnesota, and the Independent National Electoral Commission (INEC). Among these sites, the inaccessibility of INEC was of the most concern because it was inaccessible for the longest period of time, from April 12 through 14, 2007.

However, ONI researchers determined that all the sites, including INEC, were inaccessible due to technical errors in the Nigerian network. In the case of INEC, for example, the site was most likely inaccessible due to an incorrect domain name system (DNS) configuration. DNS connects a Web site's name (www.inecnigeria.org) with its IP address (66.226.64.30). If the DNS is improperly configured it will fail to connect the user to the server on which the Web site is stored and an error message will appear.

This analysis is consistent with what Nigerian experts told the field team about the technical weaknesses of the Nigerian Internet. Both the director of the Nigerian Internet Exchange and the CFO of Tara Systems told members of the field team that they were likely to come across errors due to malconfigured DNS.

Testing space in Lagos

This technical diagnosis also makes sense from a political perspective. It is highly unlikely that the regime would block a government agency, especially given that INEC, despite its name, is far from independent. Throughout the election process, Obasanjo has used INEC as a tool in his effort to rig the election in favor of his own party.[34] This included a ruling in which INEC disqualified Atiku Abubakar, one of Obasanjo's most bitter enemies, from running for president. The Nigerian Supreme Court later reinstated Abubakar's candidacy, stating that INEC did not have the right to disqualify candidates.[35] Given its reputation as a staunch ally of the ruling regime, it is highly unlikely that the INEC site was blocked by the government, furthering supporting the technical failure hypothesis.

[34] "Abuse of State Power," Human Rights Watch, http://hrw.org/backgrounder/africa/nigeria0407/6.htm

[35] "INEC to Allow Atiku Abubakar to Contest at Court's Behest," INEC Bulletin (March 14, 2007), http://www.inecnigeria.org/uploaddocs/Bulletin%20of%2014%20March%202007%20(P1).pdf.

Part 3: And so, is the Internet Under Threat in Nigeria?

Although no blocking or filtering was discovered by ONI research during the April 2007 elections, there appear to be reasons to maintain vigilance.

As mentioned in Part 1, there have been several legislative and structural changes in the Nigerian government's Internet policy. Specifically, the recent creation of the Directorate for Cybersecurity could serve as a new locus for increasing constraints on free expression over the Internet. Moreover, the Computer Security and Critical Information Infrastructure Protection Bill of 2005 could grant new Internet surveillance powers to the central government with a low level of external oversight.

The Will to Censor but Perhaps Not the Means

In Nigeria, significant obstacles to Internet blocking remain. Ironically, the Nigerian government may be foiled by their own refusal to build and maintain telecommunications infrastructure. This lack of reliable infrastructure has led those who can afford it to build their own. Most major businesses, and even many private individuals, own diesel-powered electric generators. The "do it yourself" trend applies to Internet infrastructure as well. Those who can afford the expense are opting for private satellite connections via VSAT (see Part 2) instead of Nigeria's own fiber optic and telephone infrastructure. As a result, a significant percentage of Nigeria's Internet traffic travels through infrastructure that the Nigerian government does not control, namely private communication satellites operated by independent companies in foreign countries.

The Nigerian government could theoretically filter international Internet traffic through the SAT-3 fiber optic gateway and domestic Internet traffic through the NIXP Internet exchange. Both pieces of infrastructure are located in the same building in Lagos, which is owned by Nitel.

However, because of the existence of private satellite connections, Nigeria's filtering could never be as thorough as that found in, for example, China, Iran, or Tunisia. Those who could afford satellite connections would be able to bypass filtering mechanisms on Nigeria's land-based infrastructure.

The SAT-3 fiber optic cable makes landfall in Nigeria in the Nitel headquarters in Lagos (above). The building also houses the NIXP domestic internet exchange. The building lacks a reliable power supply, modern security system, and proper climate controls for the equipment.

In order to effectively filter the Internet, the Nigerian government would have to enlist the private ISPs, mandating that they filter their clients' Internet requests. ISPs that are private companies are less reliable allies in censorship than a government agency, as their prime concern is the bottom line, not political control. This effort to engage ISPs in filtering has not been made, though the Critical Information Infrastructure Protection Bill is making movements in this direction.

Diesel generators (above) keep Nitel headquarters operational. They run 24 hours a day as the Lagos electricity grid is extremely unreliable, with outages occuring on a daily basis.

In sum, while filtering is possible along Nigeria's phone and fiber optic infrastructure, the presence of private satellite connections to the Internet presents a hurdle to comprehensive filtering.

The Importance of Monitoring the Internet around Elections

Communications tower in Lagos

The combination of possible threats to the openness of Nigeria's Internet and a history of corruption make monitoring all the more important. Projects such as the ONI may help to highlight the importance of ensuring Internet openness and could contribute to making such openness a criterion for judging the freedom and fairness of elections. While ONI research did not find evidence of filtering during the April 2007 elections, conducting this type of testing is important in establishing norms that can act against future limitations on freedom of expression on the Internet.

Part 4: Summary

Despite legitimate concerns about the openness of the Nigerian Internet, ONI research found no evidence of filtering during the April 2007 election. Although some sites were inaccessible during the testing period, these errors were ascribed to malconfigured DNS which failed to connect Web site names with their IP addresses.

Nevertheless, the Nigerian Internet may be under threat in the future. The fraud and violence perpetuated by the Nigerian government and documented by international observers, which led to voters being disenfranchised during the elections, suggests that the current leadership may be willing to go to some lengths to ensure a desired political outcome.[36] Moreover, the creation of the Directorate for Cybersecurity, along with cybercrime legislation in 2005, indicates that the Nigerian government may be interested in increasing its capacity to control the Internet.

[36] For example, see "Election or Selection?: Human Rights Abuse and Threats to Free and Fair Elections in Nigeria" Human Rights Watch, http://hrw.org/backgrounder/africa/nigeria0407/index.htm; "Election Monitoring Report," Network of Mobile Election Monitors (NMEM), eds., http://www.kiwanja.net/miscellaneous/NMEM_Election_Report.pdf. This report found that, while in some areas voting went more smoothly than in previous elections, the overall level of documented fraud indicates that there is still significant need for improvement.

Appendix: Figures for African Telecommunications Graphs

The data below was drawn from the International Telecommunication Union Yearbook of Statistics: Telecommunication Services Chronological Time Series 1995-2004, (Geneva, Switzerland: ITU, 2006).

Data for Graph 1: Growth of Cellular Phone Subscription in Africa (1995-2004)

Year	Ghana	Kenya	Morocco	Nigeria	South Africa
1995	6200	2279	30000	13000	535000
1996	12766	2826	43000	14000	953000
1997	21866	6767	74000	15000	1863000
1998	41753	10756	117000	20000	3337000
1999	70026	23757	369000	25000	5188000
2000	130045	127404	2342000	30000	8339000
2001	243797	600000	4772000	400000	10787000
2002	386775	1187122	6199000	1608000	13702000
2003	795529	1590785	7360000	3149000	16860000
2004	1695000	2546157	9337000	9147000	20839000

Data for Graph 2: Growth of Internet Users in Africa (1995-2004 estimates)

Year	Ghana	Kenya	Morocco	Nigeria	South Africa
1995	60	200	1000		280000
1996	1000	2500	1552	10000	355000
1997	5000	10000	6000	20000	700000
1998	6000	15000	40000	30000	1266000
1999	20000	35000	50000	50000	1820000
2000	30000	100000	200000	80000	2400000
2001	40000	200000	400000	115000	2890000
2002	170000	400000	700000	420000	3100000
2003	250000	1000000	1000000	750000	3325000
2004	368000	1054920	3500000	1769661	3566000