UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
February 2014

Internet Filtering in a Failed State: The Case of Netsweeper in Somalia

KEY FINDINGS

- Internet censorship products made by Canada-based Netsweeper have been identified on the networks of three Somalia-based Internet Service Providers (ISPs).
- Testing has demonstrated that the Netsweeper installation on the network of the ISP Hormuud is being used to filter content.
- The history of contested political authority and influence of a radical insurgency within Somalia raises questions about whether Netsweeper undertook due diligence before providing its filtering technology to the ISPs and telecom providers in the country.
- The finding of Netsweeper products in Somalia—a war-torn country and one of the world's most "failed states"—follows Citizen Lab prior reports finding Netsweeper products in United Arab Emirates, Yemen, Qatar, Kuwait, and Pakistan, and demonstrates a clear track record on behalf of Netsweeper of actively pursuing business opportunities for country-level filtering of countries with questionable human rights and governance practices.

INTRODUCTION

In this report, we discuss the presence of technology provided by Netsweeper—a Canada-based company that develops web filtering solutions—on the networks of three Somalia-based ISPs. We also discuss the implications of our findings in relation to human rights standards, corporate social responsibility, and international sanctions against Somalia. Internet access in Somalia is extremely limited. The country's low penetration rate can be ascribed to political volatility and economic stagnation in the context of over two decades of near continuous conflict. Despite limited connectivity, Internet growth is still predicted to increase in the future, and several Internet Service Providers (ISPs) operate in the country.

This report is a continuation of Citizen Lab's research investigating and analyzing Internet filtering and surveillance practices worldwide. It aims to inform public policy, advocacy work, and research in this field.

Prior research on use of commercial filtering technologies in problem countries

The Citizen Lab has performed extensive research on the presence of commercial filtering technologies across the globe. In 2013, Citizen Lab researchers discovered the presence of devices manufactured by Blue Coat Systems on public networks in 83 countries, including Iran and Sudan.[1] Blue Coat Systems is a California-based company that produces networking appliances capable of website filtering and deep packet inspection.[2] As part of the OpenNet Initiative,[3] the Citizen Lab identified filtering products developed by the Canada-based company Netsweeper operating on ISPs in several Middle Eastern countries, including Qatar, United Arab Emirates (UAE), Yemen, and Kuwait.[4] Two years later, the Citizen Lab found Netsweeper filtering products on Pakistani ISPs.[5] The Citizen Lab has performed similar research on SmartFilter—an American-made filtering product—and documented its presence in Saudi Arabia and the UAE.[6] The Citizen Lab also conducts research on FinFisher—a line of surveillance technology sold by the UK-based Gamma Group—and has documented the presence of FinFisher command-and-control servers in 36 countries across the world.[7]

Background about Somalia

Somalia has undergone tremendous civil strife and instability since the overthrow of President Siad Barre in 1991. Rival warlords and insurgent groups have competed for power since that time. Famine beset Somalia in 1992 and from 2010-2012. Since 2006, Somalia has faced a growing insurgency by Islamist groups such as the Islamic Courts Union (ICU) and al-Shabaab, an al-Qaeda-affiliated organization that branched out from the ICU. Piracy off the shores of Somalia has become a significant regional threat, with the costs of pirate attacks on international maritime trade in 2011 estimated to be between USD 6.6 to 6.9 billion.[8]

After the fall of the Barre regime, centralized political control effectively collapsed and a number of regions claimed autonomy from Somalia. Somaliland, Somalia's northernmost region bordering Djibouti and Ethiopia, declared itself a sovereign state in 1991. While the international community has yet to officially recognize its political autonomy, Somaliland has in effect been an independently governed state for over two decades. Mogadishu serves as the capital of the internationally recognized government of Somalia, the Federal Government of Somalia, which is comprised of an executive branch and parliament. Other regions in Somalia include Puntland, which declared autonomy in 1998 but still exists within the framework of the Somali federal system.

INTERNET IN SOMALIA

Internet access in Somalia is limited. According to an estimate by the International Telecommunications Union (ITU), Somalia's Internet penetration rate was 1.38 percent in 2012, ranking Somalia among the countries with the lowest Internet penetration in the world.[9] As of 2005, Balancing Act reported that 22 established ISPs existed in the country.[10]

The lack of a central government has permitted a wide range of businesses to operate in the country, free from taxes or service obligations that might otherwise impede growth.[11] However, the fragile political and security situation in Somalia limits the activities of many of its ISPs. Somali ISPs Somtel and Telesom, for example, operate in Somaliland.[12] Due to widespread piracy off Somalia's coastlines, most Somalis must rely on satellite rather than undersea cables to connect to the Internet globally.[13] Fear of piracy has deterred cable-laying ships from operating in Somalia's waters, thereby impeding both the development and maintenance of undersea cables.[14] The East African Marine Cable (TEAMS), for example, has been diverted an extra 200 kilometres from Somalia's coastline.[15] The largest Mogadishu-based telecommunications companies—

Nationlink, Hormuud, and Olympic—have stationed their equipment centers in Mogadishu's Bakara market, an area that has long been the site of violent struggle between the government and al-Shabaab insurgents. In 2011, Hormuud's headquarters was repeatedly hit by artillery during conflict between al-Shabaab fighters and government forces, destroying equipment and killing staff.[16]

At-home connectivity is expensive and remains unaffordable for most Somalis. Estimates in 2012 indicated that service costs for home Internet range from USD 30-600 per month depending on speed and level of service.[17] A report by the Somali Telecommunications Association (STA) in 2006 indicated that Somalia had 234 cyber cafes growing at a rate of more than 15 per cent every year.[18] Service in Internet cafes is often slow, with speeds rarely exceeding 100 kb/s.[19]

Despite these challenges, there are indications that Somalia's Internet infrastructure will improve in the near future. In 2013, satellite provider O3b Networks Ltd. signed a deal with Somtel to provide connectivity through fiber optic cables as well as satellites.[20] Liquid Telecom, a Mauritius-based telecommunications provider, announced in November 2013 that it will also partner with Hormuud to build Somalia's first terrestrial fibre-optic cable to be built across the border with Kenya.[21]

Conversely, Somalia has a robust cellular infrastructure. Several factors, including the regulatory void exploited by the telecom companies, the competing armed factions and tribal groups' heavy reliance on telecommunications infrastructure to operate their enterprises, and the telecommunications-dependent informal banking system, Hawala, used primarily by the Somali diaspora in Europe and North America to send remittances, have contributed to the thriving cellular communications market. Somalia also has an efficient mobile banking system known as ZAAD, that enables users to transfer funds, make purchase, and pay bills.[22]

In August 2012, media stories reported that Djibouti is able to restrict Internet communication in Somaliland, as the company which provides upstream Internet and telecommunications services to Telesom and Somtel is headquartered in Djibouti. A report from Somali news website Suna Times reported that the government of Djibouti ordered Telesom to block websites.[23] Citizen Lab is not able to verify whether these websites have indeed been blocked. However, technical investigation shows that as Telesom's sole transit provider, Djibouti Telecom (AS30990) would be able to exert this leverage to influence blocking in Telesom (AS37473)'s network.

Legal and regulatory frameworks

Somalia's weak central government and continuous state of instability has hindered the development of strong legal frameworks. The Fund for Peace has ranked Somalia number one on its failed state index consistently from 2008 to 2013.[24] While an internationally recognized federal government has existed since 2012, tensions between the central government and the self-declared independent state of Somaliland continue to exist.[25] The government's control of the country often does not extend beyond Mogadishu, and continuous poverty, widespread corruption, and a constant state of insecurity due to conflict with Islamist insurgents and other factions contribute to the state's failure to effectively govern Somalia.[26] The actual implementation of laws, regulations, and other statutes are therefore severely constrained in such a politically, economically, and socially fragile environment.

Somalia adopted a new constitution in August 2012 during a meeting of its National Constituent Assembly. Articles 16 and 18 of Somalia's Provisional Constitution call for Freedom of Association and Freedom of Expression and Opinions, respectively. Article 18 specifically states that "Freedom of expression includes freedom of speech, and freedom of the media, including all forms of electronic and web-based media."

Despite these guarantees, Reporters Without Borders reported that 18 members of the media were killed in 2012, and there have been at least two examples of government action against protesters in the past year.[27]

Telecommunications and media in Somalia are governed by the Somali Media Law of 2007, which guarantees "freedom of expression and ideas" and specifically outlaws censorship, stating that "The media cannot be censored and cannot be compelled to publicize information complementary neither to the government nor to the opposition."[28] However, Article 12 of the Media Law states that media outlets should "avoid broadcasting and disseminating materials jeopardizing the Islamic religion and the Somali traditional ethics, unity of Somali people and sovereignty the [sic] Somali republic," including information judged to be "false," "contrary to the religious confession and the Islamic doctrine," or "pornographic." Article 16 mandates against disseminating "fictitious information and denouncement contrary to the dignity of the Somali citizen, person, organization, business entity, or the state."

Under the Somali Media Law, the government must appoint a National Media Council (NMC) comprised of 10 members from private media and five from public media. The NMC has regulatory oversight of media outlets.

Somaliland and Puntland are governed by separate laws due to their semi-autonomous status. Media in Somaliland is governed by the Press Law of 2004, though as of 2011 stakeholders from government and media had drafted and were attempting to pass a new Law on Media & Access to Information as well as a Broadcasting Law. None of Somalia's communications laws guarantee access to information.

As of 2012, the Council of Ministers of the Transitional Federal Government had adopted the Communications Act of 2012, a draft law proposed by the Minister of Information, Posts, and Telecommunications.[29] The draft law would create the National Communications Commission (NCC), a new and independent regulatory body with jurisdiction over broadcast media and telecommunications. The NCC would reportedly be transparent, accountable, and legally bound to respect the rights of citizens to freedom of expression.

Radical groups' threat to telecommunications companies in Somalia

In January 2014, the al-Qaeda-linked al-Shabaab group issued a directive prohibiting companies from providing Internet services, and gave them fifteen days to stop the mobile and fiber optic services.[30] The group warned that those who do not comply will be considered as "working with the enemy" and will be dealt with according to Islamic law. Later that month, media reports said militants loyal to al-Shabaab began enforcing the ban in areas under their control, and that the militants were checking mobile phones for Internet connections.[31] Reports also said that all telecommunications companies in al-Shabaab-controlled regions discontinued providing Internet services on cell phones.[32] Citizens reported that telecommunications company Hormuud shut down its data service in areas under militant control.[33] The mayor of Mogadishu, Mohamud Ahmed Nur Tarsan, said militant groups forced Hormuud to shut down Internet service by threatening to kill the company's staff and senior officials in the areas controlled by al-Shabaab.[34]

The Minister of Interior and National Security of Somalia, Abdikarim Hussein Guled, condemned the al-Shabaab Internet ban, and called on the telecommunications companies to resist any coercion.[35] He also said, "The Somali Government will work with all telecommunications companies and ensure that they are free to provide Internet and other related communications services to our citizens. While the government provides all the necessary assistance to protect the public, we also caution them not to cooperate and work with terrorist groups or bow to threats. We have a responsibility to protect our citizens against all threats." The minister also said, "Our constitution guarantees freedom of expression and every citizen has the right to access information

without fear." [36] Despite al-Shabaab's Internet ban, the organization has an active presence online. Their Twitter feed remained active until the social media site banned al-Shabaab's presence after they tweeted their support for the Westgate Mall attack in Nairobi that killed 72 people.[37] Their threat against Internet providers was posted on their Facebook page.[38]

A January 2014 Gulf News article described the telecommunications operators in Somalia as pirates of airwaves, and said that they are responsible for "bedevilling successive governments" by means of tax avoidance, and preventing the current fragile government from cutting off communications to terror-linked militias.[39] "By negotiating with foreign companies to charge above the usual rates and to put money collected into overseas funds, these "companies" avoid tax—and have sufficient clout to offer deals to favoured factions, or fund groups they believe will deliver a government suited to their economic or ideological aims," the article said. The article also said the companies create wealth by "persuading other telcos worldwide to clip the ticket for them," and that they became "wealthy enough to avoid attempts by government and the regulatory International Telecommunication Union (ITU) to rein them in."

INTERNET FILTERING IN SOMALIA

Netsweeper Installation Identification Method

Citizen Lab researchers used the computer search engine Shodan[40] to scan Somali networks for evidence of installed Internet filtering devices.[41] In November 2013, these Shodan searches found the commercial filtering technology Netsweeper active on three IP addresses on networks in Somalia and Somaliland. This finding was followed up with testing for Internet filtering using software developed by Citizen Lab, which tests the accessibility of a list of sensitive URLs. The test runs were conducted in December 2013.

Netsweeper on Hormuud Telecom Somalia Inc

Scanning via search engine Shodan found a Netsweeper installation on the IP 41.78.72.114. Tests show that this device is active on the network of Hormuud Telecom Somalia Inc., as seen in Figure 1.

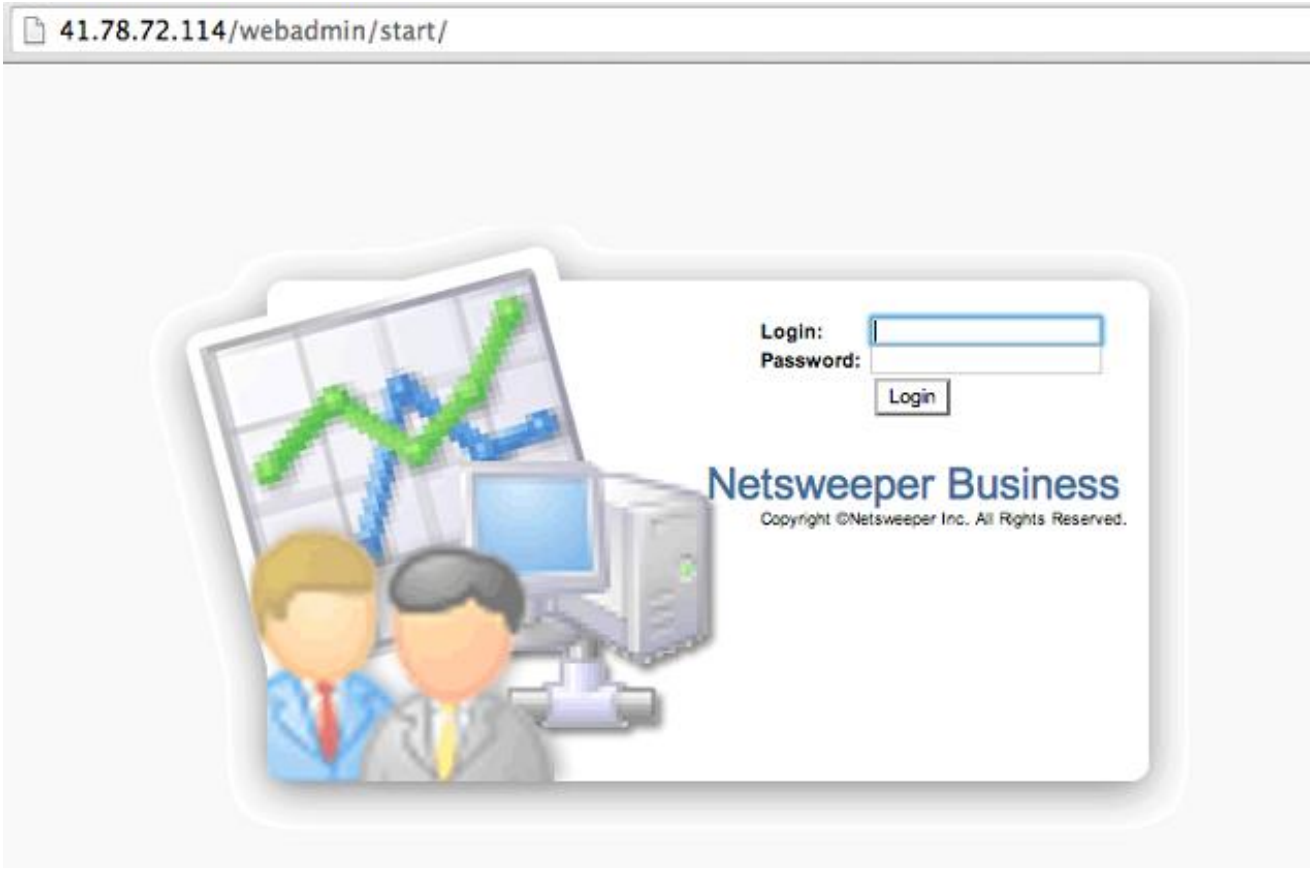

Figure 1: Screenshot of Netsweeper installation on Hormuud Telcom Somalia Inc, at http://41.78.72.114/webadmin/start/

Hormuud Telecom Somalia is one of the major telecommunications providers in Somalia. According to its website, it enjoys over 60 percent of market share in both mobile and broadband services.[42]

Netsweeper installation on Golis Telecom

A Netsweeper installation was also found installed on the network of Golis Telecom, which describes itself as the largest telecommunications operator in northeastern Somalia, offering home and business Internet services.[43]

A Netsweeper installation is active at http://113.208.81.52:8080/webadmin/start/. The index URL displays the logo of Golis Telecom Somalia, as seen in Figure 2 (http://113.208.81.52:8080/webadmin/deny/index.php).

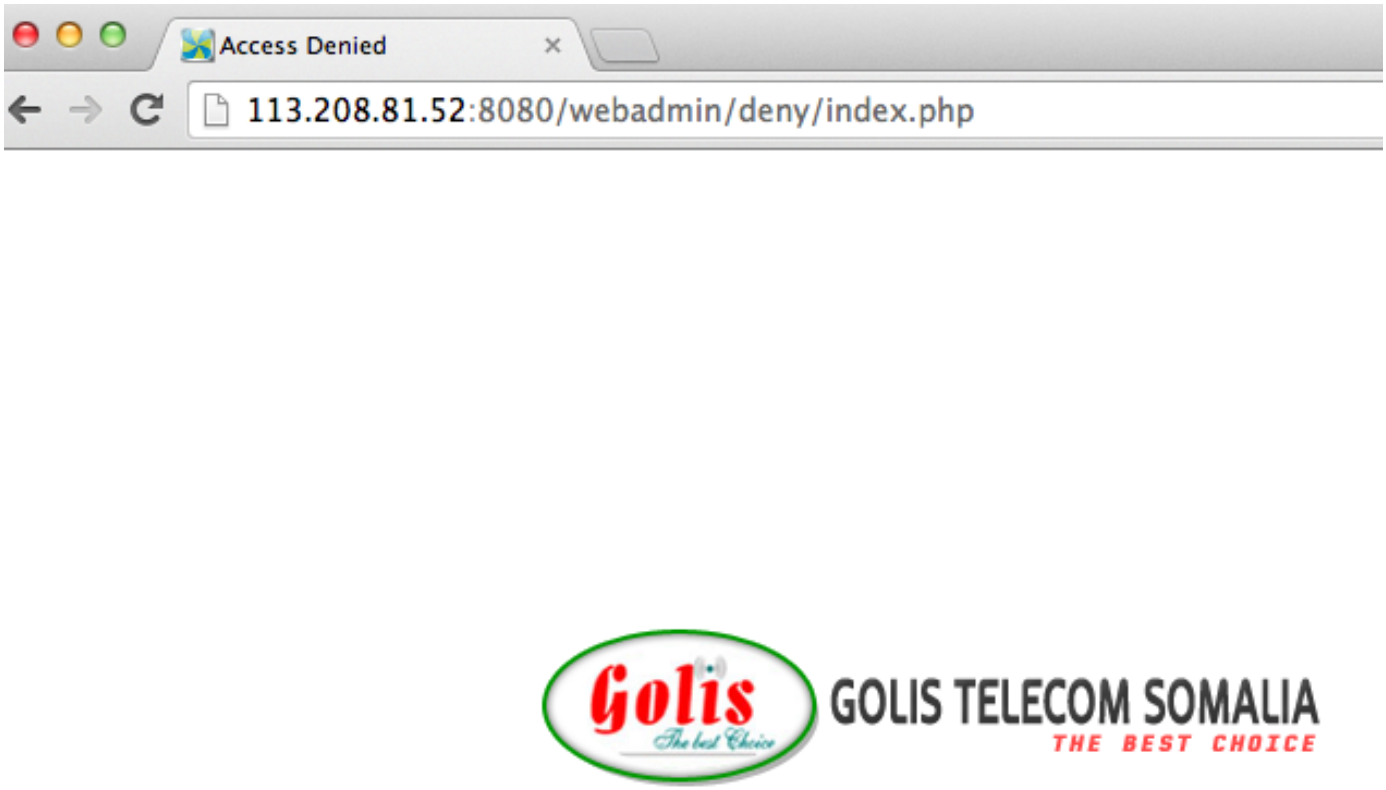

Figure 2: Screenshot of Netsweeper installation on Golis Telecom at http://113.208.81.52:8080/webadmin/deny/index.php

The IP address of this Netsweeper installation (113.208.81.52) points to host-113-208-81-052.absatellite.net, a host on the Asia Broadcast Satellite service, a company which provides VSAT services for telecommunications providers.[44] The IP address range for Golis Telecom (41.223.110.0/24) is announced by ASN 45572, also on the Asia Broadcast Satellite service.

Netsweeper on ISP Telesom

Netsweeper is also installed on telecommunications company Telesom at control panel http://197.157.246.196:8080/webadmin/start/ [See Figure 3]

Telesom is a telecommunications company headquartered in Hargeisa, the capital of Somaliland. It provides broadband Internet and mobile communication products.[45] Accessing the 'webadmin/deny' URL seen below in Figure 3 displays a Golis Telecom logo. It is not clear why this page displays the logo of Golis instead of the Telesom logo, although Telesom lists both Golis Telecom and Hormuud as partners.[46]

Figure 3: Screenshot of Netsweeper installation on Telesom Somaliland at http://197.157.246.196:8080/webadmin/deny/

Test Results

A short list of 49 URLs was tested in the country as a means of confirming the presence of Internet filtering and the use of Netsweeper technology to implement that filtering. Testing was conducted in December 2013 on Somalia's networks through the use of a specially designed measurement client. This client accesses a pre-defined short list of 49 URLs on Somali networks while simultaneously triggering tests of the same URLs from a control location at the University of Toronto, which does not censor the type of content for which the client tested. The results of these tests are sent by the measurement client to servers at the University of Toronto for analysis.

We were not able to run full test runs from inside the country because of our security concerns over the threats by the al-Shabaab organization to Internet companies and users. Our concern for the security of potential in-country testers prevented us from extensive testing, so there may be websites and content categories beyond those identified here which are blocked. We have tested on one of the ISPs (Hormuud) identified above as potentially having an active Netsweeper device used to filter content. A full list of tested URLs can be found in the 'Data' section below.

Hormuud

Two tests of the 49 URL testing list were run in December 2013. In total, nine URLs were found to be blocked: seven pornography URLs and two URLs of circumvention/anonymizer tools. The following URLs were found to be blocked using the method described below:

URL	Category
http://fuck.com	Pornography
http://hidemyass.com	Anonymizers/Circumvention
http://peacefire.org	Anonymizers/Circumvention
http://playboy.com	Pornography
http://porn.com	Pornography
http://sex.com	Pornography
http://torproject.org	Anonymizers/Circumvention
http://www.proxy4free.com/list/webproxy1.html	Anonymizers/Circumvention
http://xhamster.com	Pornography

The method of blocking can be seen in the following example of an attempt to access the circumvention site http://peacefire.org: (Note: data referring to the IP address of the tester has been anonymized)

GET / HTTP/1.1
Accept-Encoding: identity
Host: peacefire.org
Connection: close
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1)
HTTP/1.0 302 Moved
Content-Length: 0
Location: http://41.78.72.114:8080/webadmin/deny/index.php?dpid=75&dpruleid=54&cat=32&ttl=-200&groupname=default&policyname=default&username=-&userip=41.78.X.X&connectionip=1.0.0.127&nsphostname=netsweeper2.hortel.net&protocol=nsef&dplanguage=-&url=http%3a%2f%2fpeacefire%2eorg%2f
Pragma: no-cache
Cache-Control: no-cache

As seen in this exchange, the user is redirected through HTTP code 302 to a blockpage. This redirection is injected into the GET request response, as the legitimate response from the server is also present in packet captures from the tests of URLs which are blocked. The HTML of this blockpage can be seen in this example of an attempt to access peacefire.org:

```
<!DOCTYPE html PUBLIC “-//W3C//DTD XHTML 1.0 Transitional//EN”
“http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd”>
<html>
<head>
<title>Untitled document</title>
</head>
<body>
<p>              &n
bsp;              &n
bsp; <img src=”http://peacefire.org/webadmin/deny/images/hormuud_block_page.JPG” alt=”” /></p>
</body>
</html>
```

The blockpage attempts to load the image ‘http://[tested URL]/webadmin/deny/images/hormuud_block_page.JPG’, where [tested URL] is the URL being tested, instead of opening it from a Hormuud hosted site. This will prevent the correct image from loading, and appears to be the result of a misconfiguration. However, the correct blockpage can be viewed by replacing [tested URL] with the IP address found via Shodan, as seen below in Figure 4.

Figure 4: Blockpage on ISP Hormuud Telecom Somalia at http://41.78.72.114

The format of this blockpage URL is consistent with the use of Netsweeper devices.[47] In addition, the original redirect explicitly refers to Netsweeper (‘netsweeper2.hortel.net’).

Mapping the ASNs of three telecommunication networks in Somalia shows that telecommunications companies Hormuud, Telesom, and SomCable are gateways to Internet connections from and to Somalia. Hence, the installation of Netsweeper filtering technology on Hormuud and Telesom is significant giving their strategic positions; these networks are not just local providers or resellers, but rather among the telecom providers that exert the leverage of shaping and controlling Internet traffic and information flow into and out of the entire country [Figure 5].

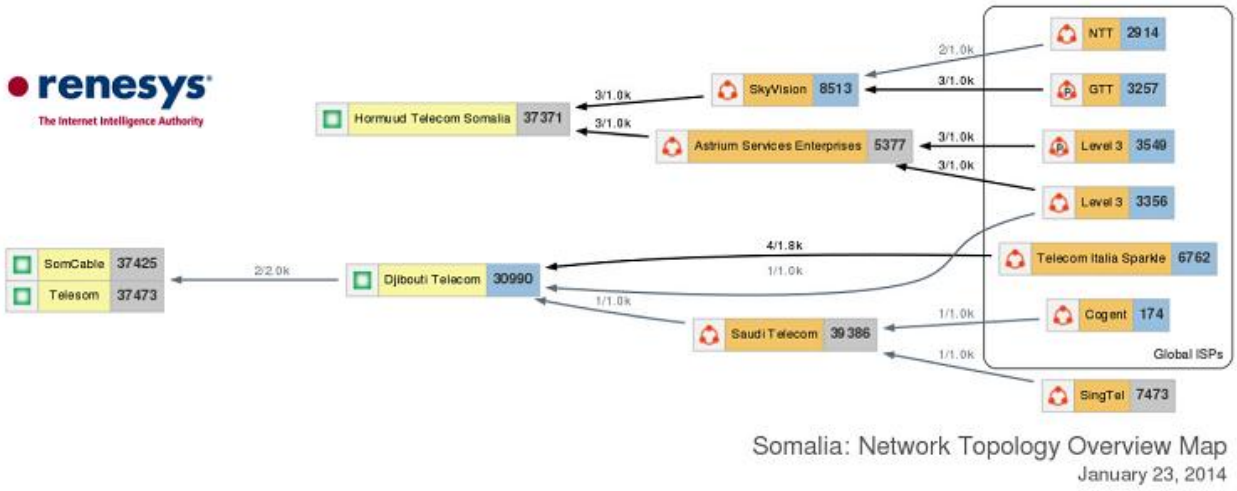

Figure 5: Map of network connectivity of 3 ISPs in Somalia. Image courtesy Doug Madory at Renesys.

DISCUSSION

The presence and use of commercial Internet filtering technologies in countries with poor records of human rights practices have always raised questions about the ethical practices of the providers of such technologies. The presence and use of Netsweeper in Somalia raise even more interesting questions and present a number of avenues for future research. At one time, the United Nations Security Council imposed sanctions against Ali Ahmed Nur Jim'ale, identified as controlling owner of Hormuud.[48] Although that no longer is the case, the history of concern around telecommunications companies and radical insurgency in Somalia is, to say the least, complex and begs the following questions:

How and why did a Canadian-made filtering technology end up on the networks of these telecommunications companies in a country ranked as the most failed state on earth? Somalia's weak central government, autonomous regions and ongoing insurgency mean that authority is contested amongst a number of actors. Did Netsweeper Inc. undertake due diligence before providing its filtering technology to the ISPs and telecom providers in Somalia? Has Netsweeper assessed if its products will be used in Somalia in ways that violate internationally recognized human rights norms and principles, and to prevent the receiving and imparting of information protected by Article 19 of the Universal Declaration of Human Rights? More importantly, are the telecommunications companies in Somalia using Netsweeper technology to implement filtering policies enforced by radical groups?

In this report, we were not able to document the full breadth and scope of what content is filtered on Hormuud and whether the Netsweeper installations present on Golis and Telesom are also being used to filter content. In addition, further research could examine what types of content are filtered beyond the pornography and circumvention tool websites identified here.

In our June 2013 report,[49] which outlines the use of Netsweeper technology to engage in censorship of political and social content on the Pakistani ISP Pakistan Telecommunication Company Limited, we posed a number of questions to Netsweeper and committed to publishing their response in full. As of this report's publication date, we have not received a response to these questions. The same set of questions are applicable in the case of Somalia.

- Does Netsweeper have a human rights policy, and does it implement this policy when developing its technologies and sales strategy?
- Does the company assess the human rights impact of its products during the design phase and has it ever discarded or altered designs given their inherent capability to undermine rights of freedom of expression and access to information?
- What resources does Netsweeper devote to human rights programs at the operational level? Does Netsweeper ask staff in relevant departments (e.g., legal, sales, engineering) to undergo human rights training?
- Is Netsweeper aware of the "know your customer" standard, where companies actively investigate whether potential clients may use technology to undermine human rights standards? If so, how does it implement this standard (for example, through active investigation of a government's human rights record)?
- Has Netsweeper implemented the United Nations Guiding Principles on Business and Human Rights (the so-called "Ruggie Principles") in building a business strategy that safeguards human rights standards?
- Has Netsweeper explored joining the Global Network Initiative (GNI), a network of business, civil society, and academic stakeholders, in finding solutions for technology companies to uphold standards of privacy and free expression, as the ICT company Websense did in 2011?

We commit to publishing Netsweeper's reply in full.

DATA

A complete list of URLs tested in Somalia in December 2013 can be found here:

- [CSV]

ACKNOWLEDGEMENTS

The Citizen Lab would like to thank Matt Bryden (Chairman of Sahan Research) and Aisha Ahmad (Assistant Professor, Department of Political Science, University of Toronto) for valuable input into this report, and Doug Madory from Renesys for producing the maps of ASNs in Somalia.

FOOTNOTES

[1] Morgan Marquis-Boire, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton, "Some Devices Wander by Mistake: Planet Blue Coat Redux," Citizen Lab, July 9, 2013, accessed February 14, 2014, https://citizenlab.org/2013/07/planet-blue-coat-redux.
[2] Ellen Nakashima, "Report: Web Monitoring Devices Made by U.S. Firm Blue Coat Detected in Iran, Sudan," Washington Post, July 8, 2013, accessed February 14, 2014, http://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html.
[3] The Citizen Lab is a founding partner of the OpenNet Initiative project, which seeks to investigate, expose and analyze Internet filtering practices in a credible and non-partisan fashion. For more information see OpenNet Initiative, https://opennet.net.
[4] Helmi Noman, "When a Canadian Company Decides What Citizens in the Middle East Can Access Online," OpenNet Initiative, May 16, 2011, accessed February 16, 2014, https://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online.

[5] "O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime," Citizen Lab, June 20, 2013, accessed February 16, 2014, https://citizenlab.org/2013/06/o-pakistan.
[6] Bennett Haselton, "Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE," Citizen Lab, November 28, 2013, accessed February 16, 2014, https://citizenlab.org/2013/11/smartfilter-miscategorization-filtering-saudi-arabia-uae.
[7] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri and John Scott-Railton, "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, April 30, 2013, accessed February 16, 2014, https://citizenlab.org/2013/04/for-their-eyes-only-2.
[8] Venetia Archer and Robert Young Pelton, "Can We Ever Assess the True Cost of Piracy?" Somalia Report, February 21, 2012, accessed February 16, 2014, http://www.somaliareport.com/index.php/post/2867/Can_We_Ever_Assess_the_True_Cost_of_Piracy_.
[9] "Percentage of Individuals Using the Internet," International Telecomunications Union, accessed February 16, 2014, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.
[10] "Somalia's Civil War Hides Steady Growth of Internet," Balancing Act, accessed February 16, 2014, http://www.balancingact-africa.com/news/en/issue-no-345.
[11] "Somalia – Telecoms, Mobile and Broadband," BuddeComm, accessed February 15, 2014, http://www.budde.com.au/Research/Somalia-Telecoms-Mobile-and-Broadband.html
[12] "About Telesom," Telesom, accessed February 16, 2014, http://www.telesom.net/index.php/about-us; and "Who We Are," Somtel, accessed February 16, 2014, http://somtelnetwork.net/home/whoweare.
[13] Juliet Onyango, "Somalia to Access High-Speed Internet," Zegabi, November 15, 2013, accessed February 16, 2014, http://www.zegabi.com/articles/?p=5556.
[14] Somali Pirates Hold Back Seacom Cable, new opening date is 23 July," Balancing Act, June 26, 2009, accessed February 16, 2014, http://www.balancingact-africa.com/news/en/issue-no-460/internet/somali-pirates-hold/en.
[15] "Navies to Guard Undersea Cable From Somali Pirates," Reuters, April 16, 2014, accessed February 16, 2014, http://www.reuters.com/article/2009/04/16/idUSLG73912.
[16] "SOMALIA: Internet Lifeline Cut in Mogadishu," IRIN, May 27, 2011, accessed February 16, 2014, http://www.irinnews.org/report/92824/somalia-internet-lifeline-cut-in-mogadishu.
[17] "Internet Accessibility Growing Steadily in Somalia," Hiiraan Online, October 15, 2012, accessed February 16, 2014, http://www.hiiraan.com/news4/2012/Oct/26384/internet_accessibility_growing_steadily_in_somalia.aspx.
[18] Jonathan Kalan, "Somalia's Ambitions Online Could Bring Mogadishu to the World," BBC, October 23, 2012, accessed February 15, 2014, http://www.bbc.co.uk/news/business-19961266.
[19] "Internet Accessibility Growing Steadily in Somalia," Hiiraan Online, October 15, 2012, accessed February 16, 2014, http://www.hiiraan.com/news4/2012/Oct/26384/internet_accessibility_growing_steadily_in_somalia.aspx.
[20] Chris Spillane, "Somalia to Get High-Speed Internet After Satellite Deals," Bloomberg, November 13, 2013, accessed February 14, 2014, http://www.bloomberg.com/news/2013-11-13/somalia-to-get-high-speed-internet-after-satellite-deals.html
[21] "Somalia Gets First Fibre Link From Liquid Telecom," My Broadband, November 12, 2013, accessed February 16, 2014, http://mybroadband.co.za/news/broadband/91589-somalia-gets-first-fibre-link-from-liquid-telecom.html.
[22] Ronald Deibert, Black Code: Inside the Battle for Cyberspace (Toronto: McClelland & Stewart, 2013).
[23] "Djibouti Blocks a Popular Somali Websites-Anonymous," Suna Times, August 20, 2012, accessed February 16, 2014, http://www.sunatimes.com/view.php?id=2127.
[24] "Failed States Index Five-Year Trends, 2008-2013," FFP, accessed February 16, 2014, http://ffp.statesindex.org/fsi-trends-2013

[25] "Can't Get No Recognition," The Economist, January 9, 2014, accessed February 14, 2014, http://www.economist.com/blogs/baobab/2014/01/somaliland.
[26] Ahmad Rashid Jamal, "Identifying Causes of State Failure: The Case of Somalia," Atlantic-Community.org, accessed February 16, 2014, http://www.atlantic-community.org/documents/10180/280d1fa4-ccd0-43fa-af90-834e3b2bb9b3.
[27] News Providers Decimated in 2012," Reporters Without Borders, December 19, 2012, accessed February 16, 2014, http://en.rsf.org/2012-journalists-netizens-decimated-19-12-2012,43806.html.
[28] "Somali Media Law," Somali Republic The Transitional Federal Government Ministry of Information, available at http://www.article19.org/data/files/pdfs/laws/somalia-media-law.pdf
[29] "Somalia: Draft Communications Act," Article 19, March 2012, accessed February 16, 2014, http://www.article19.org/data/files/medialibrary/3016/12-04-03-LA-somalia.pdf.
[30] "Somalia's Al-Shabab Militants Issue Internet Ban," BBC News, January 9, 2014, accessed February 14, 2014, http://www.bbc.co.uk/news/world-africa-25666470.
[31] Abdulkadir Khalif, "Somali Islamists Start Enforcing Internet Ban," Africa Review, January 23, 2014, accessed February 14, 2014, http://www.africareview.com/News/Somali-Islamists-start-enforcing-Internet-ban/-/979180/2157090/-/5xl1fcz/-/index.html.
[32] "Telecom Companies Officially End Mobile Internet Services in Al-Shabaab Held Territories Today," Harar24 News, January 22, 2014, accessed February 16, 2014, http://harar24.com/?p=11724.
[33] "Phone Data Cut After Somali Militant Threat," Associated Press, January 25, 2014, accessed February 16, 2014, http://hosted2.ap.org/APDEFAULT/cae69a7523db45408eeb2b3a98c0c9c5/Article_2014-01-25-Somalia-Militants-Internet/id-e010f0ae7a0943ce922855c120c41a0d.
[34] "Somalia: Mogadishu Mayor Says Local Companies Forced to Shut Down Mobile Internet Service," RBC Radio, February 9, 2014, accessed February 15, 2014, http://www.raxanreeb.com/2014/02/somalia-mogadishu-mayor-says-local-companies-forced-to-shut-down-mobile-internet-service/.
[35] "Somalia: Somali Minister of Interior Condemns Al Shabaab Internet Ban and Calls On Telecommunications Companies to Resist Any Coercion," All Africa, January 11, 2014, accessed February 14, 2014, http://allafrica.com/stories/201401120125.html.
[36] Office of the Minister, "Somali Minister of Interior Condemns Al Shabaab Internet Ban and Calls on Telecommunications Companies to Resist Coercion," Somali Republic Federal Government, January 11, 2014, accessed February 16, 2014, http://mad.ly/d71464.
[37] Jillian C. York, "Mine, Not Thine: Somalia's Al Shabaab Bans the Internet," Electronic Frontier Foundation, January 10, 2014, accessed February 15, 2014, https://www.eff.org/deeplinks/2014/01/somalias-al-shabaab-bans-internet.
[38] Faith Karimi, "Somalia Warns Telecom Companies Not to Comply With Al-Shabaab Internet Ban," CNN, January 11, 2014, accessed February 16, 2014, http://www.cnn.com/2014/01/11/world/africa/somalia-shabaab-internet-shutdown/.
[39] Steve Liddle, "Somalia's Other Pirates—The Telecom Companies," Gulf News, January 16, 2014, accessed February 15, 2014, http://gulfnews.com/news/region/somalia/somalia-s-other-pirates-the-telecom-companies-1.1278269.
[40] The Shodan search engine provides information on devices connected to the Internet, including industrial control systems, web filtering, and network security and optimization products. See "Locate Any Devices That's Connected to the Internet," Shodan, accessed February 16, 2014, http://www.shodanhq.com/help/tour.
[41] Citizen Lab has conducted similar investigations of commercial filtering technology using Shodan. See "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," Citizen Lab, January 15, 2013, accessed February 16, 2014, https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools.
[42] "About Us," Hormuud Telecom, accessed February 16, 2014, http://hortel.net/viewpage.php?page_id=1.
[43] "Internet Service," Golis Telecom Somalia, accessed February 16, 2014, http://golistelecom.com/en/our-services/internet-service.

[44] "Data Services," Asia Broadcast Satellite, accessed February 16, 2014, http://www.absatellite.net/services/telecommunications-data-services/#num3
[45] Telesom, http://www.telesom.net.
[46] "Member Access: Coverage & Network," Telesom, accessed February 14, 2014, http://www.telesom.net/index.php/services/mobile-services/17-company-portfolio/28-coverage-network.
[47] Masashi Crete-Nishihata, Jakub Dalek, Ronald Deibert, Phillipa Gill, Bennett Haselton, Helmi Noman, and Adam Senft, "A Method for Identifying and Confirming the Use of URL Filtering Products for Censorship," Proceedings of the 2013 Conference on Internet Measurement Conference, http://dl.acm.org/citation.cfm?id=2504763: 23-30.
[48] "Security Council Committee on Somalia and Eritrea Adds One Individual to List of Indivudals and Entities," United Nations Security Council, February 17, 2012, accessed February 16, 2014, http://www.un.org/News/Press/docs/2012/sc10545.doc.htm.
[49] "O Pakistan, We Stand on Guard for Thee," Citizen Lab. https://citizenlab.org/2013/06/o-pakistan/