



UNIVERSITY OF  
TORONTO

MUNK  
SCHOOL  
OF  
GLOBAL  
AFFAIRS

# Information Controls during Military Operations

---

## THE CASE OF YEMEN DURING THE 2015 POLITICAL AND ARMED CONFLICT

21 October 2015

Jakub Dalek (Citizen Lab), Ronald Deibert (Citizen Lab), Sarah McKune (Citizen Lab), Phillipa Gill (Stony Brook University), Naser Noor (Independent Researcher), and Adam Senft (Citizen Lab)

## Key Takeaways

---

- This report provides a detailed, mixed methods analysis of Information controls related to the Yemen armed conflict, with research commencing at the end of 2014 and continuing through October 20, 2015.
- The research confirms that Internet filtering products sold by the Canadian company Netsweeper have been installed on and are presently in operation in the state-owned and operated ISP YemenNet, the most utilized ISP in the country.
- Netsweeper products are being used to filter critical political content, independent media websites, and all URLs belonging to the Israeli (.il) top-level domain.
- These new categories of censorship are being implemented by YemenNet, which is presently under the control of the Houthis (an armed rebel group, certain leaders and allies of which are targeted by United Nations Security Council sanctions).
- We identify disruptions to infrastructure, such as electricity and fuel, as an important component of information controls in the conflict. Although we are unable to attribute specific disruptions to parties responsible, we find that on balance the limited access to information brought about by the disruptions favours the interests of the Houthis.
- Network measurements tests undertaken in Saudi Arabia and Iran show that there is a significant international “spillover” of information controls among state parties to the conflict; both states have blocked websites related to their opponents in the ongoing political and military conflicts.

## Detailed Summary

---

Recent political conflicts and periods of violent unrest -- such as those in [Syria](#), [Thailand](#), and [Iraq](#) -- have demonstrated the ways in which information and communications often become a focal point of contestation during a crisis. As information becomes a critical factor in a conflict, information controls -- which we define as *actions conducted in or through information and communication technologies that seek to deny, disrupt, secure, or monitor information for political ends* -- may increase in scope, intensity, and depth. Authorities may introduce new types of censorship as a means of preventing information from leaving the country, or in some cases even cut off access to communications entirely, such as the Internet or mobile phones services. Service providers may be required to undertake emergency measures to control information or communications, or suspend services because of violence, loss of personnel, or disruptions to their infrastructure. Contests over information controls can also become “internationalized” as outside parties to the conflict, including neighboring states, companies, non-state groups, and civil society, get involved and take action that impacts the information environment in the zone of conflict and beyond.

This report presents research on information controls in the context of the ongoing Yemeni armed conflict. After months of crisis following the September 2014 Houthi rebel takeover of the capital Sana’a, the situation in Yemen degenerated into ongoing violent conflict. The conflict has expanded since 2014 to include a military response from a coalition of Arab states led by neighbouring Saudi Arabia.

Using a combination of network measurement tests, reference to technical data sources, as well as contextual and in-country field research, we undertook a detailed examination of information controls related to the Yemeni armed conflict from the end of 2014 to October 2015. Our research was guided by the following framing questions:

- How is access to infrastructure, including basic electricity and fuel, a component of information control in Yemen’s armed conflict? Do disruptions to infrastructure favour one side of the conflict over others? Can we attribute disruptions to infrastructure to specific parties to the armed conflict?

Citizens’ ability to access information has been significantly impacted by the ongoing violence, with deliberate power outages and shortages of fuel used to power generators further weakening the country’s infrastructure. Citizens are unable to power their computers, TVs, or mobile phones. These disruptions have limited citizens’ ability to communicate with their families, keep abreast of news related to local developments, or receive advance warning from Saudi-led coalition forces to leave their homes prior to

airstrikes in active military conflict zones. The disruptions, though difficult to attribute to any particular group, favour the Houthis who have a demonstrated interest in restricting information flow.

- What other techniques of information control factor into the Yemen armed conflict?

Information controls in Yemen have taken different forms. The Houthi rebels have banned domestic telecommunication providers from sending news updates generated by local and regional media to subscribers. They have raided and shut down TV channels and radio stations, arrested journalists, raided newspaper offices, and blocked websites of local and regional media. We also take note of numerous reports of digital surveillance, but were unable to draw positive conclusions about the veracity of these reports or map Yemen's surveillance infrastructure.

- Is Internet censorship a factor in the armed conflict? Have Yemen's Internet content filtering practices shifted substantially, and if so how? How transparent is the filtering?

We find that information controls implemented by Yemen's national ISP, [YemenNet](#), a state-owned and operated national ISP that has served the entire country since 2001, and which is now controlled by the Houthi rebels, have changed substantially since the Houthi takeover of the capital and, by extension, control over the Ministry of Communications and Information Technology. Content filtering now includes a wide variety of political content, and blocking of the entire .il (Israel) domain. We also determine that all political filtering that targets local and regional news and media content is undertaken in a non-transparent way, with fake network error pages delivered back to users instead of block pages.

- What equipment is used for content filtering? Can we identify the manufacturer of filtering services? Did that company undertake any due diligence around providing services to a country in the midst of an armed conflict, and to ISPs now under the control of a group (the Houthis) whose leaders are subject to UN Security Council sanctions?

Our [prior research](#) on Yemen (as part of the OpenNet Initiative) identified Websense, and later Netsweeper, as commercial providers of content filtering services and equipment to Yemen's ISPs. In our latest research, we are able to positively verify that Netsweeper is still provisioning services to YemenNet. We also conducted an experiment confirming that Netsweeper is actively updating Netsweeper installations in the country, and thus knows or has reason to know of the recent expansion of the filtering regime to include political content linked to the conflict and the Houthi takeover. As part of the research for this report, on

October 9, 2015 we sent a letter to Netsweeper regarding its provision of services to YemenNet and its human rights due diligence. As of the date of publication, we have not received a reply.

- Have information controls been “internationalized” as part of the Yemen armed conflict?

In [prior research](#), we have observed that information controls can “spill out” of a particular conflict and affect access to the Internet in other countries. To continue this line of inquiry, we undertook network measurements in Saudi Arabia and Iran. We find that Saudi Arabia has implemented new Internet content filtering aligned with its military operations in Yemen. We also find that there is significant similarities between content filtering undertaken in Iran and that which has been implemented in Yemen since the Houthi takeover.

Our report begins with background to Yemen and the armed conflict, as well as to the history of information controls in the country. Part 1 provides a summary examination of information controls around the armed conflict based on contextual and field research. Part 2 presents the findings of the network measurement tests we undertook for Internet content filtering in Yemen, Saudi Arabia, and Iran, and details experiments we undertook to confirm Netsweeper’s provision of services in Yemen. We evaluate Netsweeper’s provision of services on the basis of existing human rights laws and norms, and provide details on questions we sent to the company. We conclude the report with observations on research on information controls in armed conflict in general, and the Yemen case in particular.

# Full Report: Background

---

## 2015 Political and Armed Conflict

Yemen is strategically located on the Bab al-Mandab strait, which links the Red Sea with the Gulf of Aden and is a passage for much of the world's oil shipments. However, [power struggles](#) and unequal access to resources have frequently led to violent conflict and instability in the country -- the poorest in the Middle East with a weak governance system and widespread corruption. Yemen has also been the base for attacks staged by the militant Islamist group al-Qaeda in the Arabian Peninsula (AQAP), posing a security threat at the regional and international levels. There have been six armed conflicts between the government of former president Ali Abdullah Saleh and the Shiite Houthi rebels, also known as Ansar Allah (Partisans of God), from 2004 until a ceasefire was signed in 2010. Saleh was removed from power in 2011 following popular uprisings in which the Houthis participated. Taking advantage of the vacuum created afterwards, the Houthis expanded their power to more provinces outside their stronghold Saada, and eventually seized control of the government.

Subsequent to this power shift, former President Saleh allied himself with the Houthis. A letter from the United Nations Panel of Experts on Yemen, established pursuant to Security Council resolution 2140, [notes](#) that interlocutors informed the panel that "despite waging six wars against the Houthi movement in the north of the country between 2004 and 2010," Saleh has "aligned himself with the Houthis to destroy the power base and property of his enemies," "ordered his supporters in the Government, the security services and the tribes not to intervene and curb Houthi forces in the achievement of their goals," and that "Saleh was seeking revenge against these people for contributing to his loss of power in 2011 and 2012" (para. 80).

Yemeni President Abd-Rabbu Mansour Hadi, who took power after Saleh's departure in 2011, and his government submitted their resignations in January 2015 after the Houthis expanded their control by force over the country. The Houthis then [put the president and government cabinet members under house arrest](#). In February 2015, the Houthis unilaterally announced a constitutional declaration that [dissolved parliament and formed a "revolutionary committee"](#) chaired by Mohammed al-Houthi, a relative of the group's leader Abdulmalik al-Houthi. The Houthi-led revolution committee [became](#) the de facto government and Houthis the de facto rulers running the country.

On March 27, 2015, Saudi Arabia formed and led a coalition of Arab states in launching airstrikes in Yemen against the Houthi rebel group as it continued to take over more parts of the country, including the capital Sana'a. The [coalition of states included](#) majority Sunni Muslim countries United Arab Emirates, Kuwait,

Bahrain, Qatar, Jordan, Morocco, Sudan, and Egypt. The coalition considered the Houthis, who are Shiite Muslims, to be proxies for the Shiite government of Iran, which condemned the military intervention. The coalition also imposed a naval [blockade](#) of ports in Yemen at the end of March, restricting imports including food and other basic necessities, which has [contributed to the humanitarian crisis](#) in the country.

Adel al-Jubeir, the Saudi ambassador to the United States, [said when announcing the start of the military intervention](#): "This is really a war to defend the legitimate government of Yemen and protect the Yemeni people from takeover by a radical militant group aligned with Iran and Hezbollah." The military intervention was requested by President Hadi, who had [fled the country to the Saudi capital city of Riyadh](#) after the Houthis and their allies advanced to the city of Aden, in southern Yemen, where he had taken refuge.

The Houthis warned against the coalition military operation in Yemen, saying president Hadi's request for military intervention could lead to civil war and that the operation is a "[conspiracy against Yemen and proves Hadi is a traitor](#)." An official from the General People's Congress (GPC) led by former President Saleh -- an ally of the Houthis -- [criticized President Hadi's move, saying](#) "Yemenis will reject any interference because it will bring more problems than solutions."

The United Nations Security Council (UNSC) has taken action concerning the situation in Yemen. In February 2014 the UNSC adopted [resolution 2140](#) under Chapter VII of the UN Charter, in which it expressed "concern at the ongoing political, security, economic and humanitarian challenges in Yemen, including the ongoing violence," and decided that all UN member states must enact an assets freeze and travel ban against individuals designated by a newly established sanctions committee (the "2140 Committee") as "engaging in or providing support for acts that threaten the peace, security or stability of Yemen." The measures implemented in that resolution were renewed and extended in February 2015 in [resolution 2204](#). Also in February 2015, the UNSC expressed grave concern in its [resolution 2201](#) over escalating violence and other actions of the Houthis, noting as well its concern over "the takeover by the Houthis of state media outlets and reject[ing] the use of the media to incite violence."

Shortly thereafter, in its [resolution 2216](#) of April 2015, the UNSC demanded that "all parties in the embattled country, in particular the Houthis, immediately and unconditionally end violence and refrain from further unilateral actions that threatened the political transition." It further demanded that the Houthis "refrain from any provocations or threats to neighbouring States, release the Minister for Defence, all political prisoners and individuals under house arrest or arbitrarily detained, and end the recruitment of children." Additionally, the UNSC decided that member states would expand sanctions to include an arms embargo against designated individuals, and named additional persons to the 2140 Committee's list.

The [list established and maintained by the 2140 Committee](#) currently designates the following individuals, whom the UNSC and the 2140 Committee have found to threaten the peace, security, or stability of Yemen:

- Former President Ali Abdullah Saleh, who, “[a]s of fall 2012, . . . had reportedly become one of the primary supporters of violent [Houthi] actions in northern Yemen. More recently, as of September 2014, Saleh has been destabilizing Yemen by using others to undermine the central government and create enough instability to threaten a coup. . . . The September 2014 United Nations Panel of Experts report on Yemen also states that allegations have been made that Ali Abdullah Saleh has been using Al-Qaida in the Arabian Peninsula (AQAP) operatives to conduct assassinations and attacks against military installations in order to weaken President Hadi and create discontent within the army and broader Yemeni population” ([2140 Committee narrative summary of reasons for listing](#)).
- Ahmed Ali Abdullah Saleh, the son of former President Saleh, who “has been working to undermine President Hadi’s authority, thwart Hadi’s attempts to reform the military, and hinder Yemen’s peaceful transition to democracy” ([UNSC resolution 2216](#), Annex).
- Abdulmalik al-Houthi, who “assumed the leadership of Yemen’s Houthi movement in 2004 after the death of his brother, Hussein Badreddin al-Houthi. As leader of the group, al-Houthi has repeatedly threatened Yemeni authorities with further unrest if they do not respond to his demands and detained President Hadi, Prime Minister, and key cabinet members” ([UNSC resolution 2216](#), Annex).
- Abdullah Yahya al Hakim, the “[Houthi] group second-in-command,” who “reportedly held a meeting in order to plot a coup” against Yemeni President Hadi and commanded forces that engaged in violent takeovers in the country; in late 2014 his role was to “organize military operations so as to be able to topple the Yemeni Government, and he was also responsible for securing and controlling all routes in and out of Sana’a” ([2140 Committee narrative summary of reasons for listing](#)).
- Abd al-Khaliq al-Huthi, a “[Houthi] military commander” who “led a group of fighters dressed in Yemeni military uniforms in an attack on locations in Dimaj, Yemen. The ensuing fighting resulted in multiple deaths.” Moreover, “unknown number of unidentified fighters allegedly were prepared to attack diplomatic facilities in Sana’a, Yemen, upon receiving orders from the Abd al-Khaliq al-Huthi” ([2140 Committee narrative summary of reasons for listing](#)).

UN member states have enacted sanctions against these designated individuals reflecting the UNSC resolutions. [Canada](#), the [United States](#), and the [European Union](#), among others, have all implemented Yemen-related sanctions.

As the armed conflict continues to escalate, the UN sponsored [peace talks on the conflict in Yemen](#) in Geneva in June 2015 between delegations from President Hadi and the Houthi rebels. The talks, however, [failed to produce a ceasefire](#).

In July 2015, the Saudi-led coalition [successfully pushed Houthi forces](#) from the strategic southern port city of Aden, which permitted both the [first delivery of food aid to Aden's port](#) and the [first flights to land at Aden airport](#) since March 2015. The re-capture of Aden appeared to mark a turning point in the conflict, as coalition forces began [preparing to advance on the Houthi-controlled capital of Sana'a](#). Troops from [numerous coalition countries began to arrive near the city of Marib](#) to participate in military operations there, in advance of operations on Sana'a. By the first week of September 2015, coalition [airstrikes had escalated in Sana'a](#) following a Houthi-led attack that killed 60 coalition soldiers in Marib.

In the midst of the military build-up, both sides agreed on September 11, 2015 to [engage in United Nations-mediated peace talks](#) the following week. The talks [aimed](#) to "create a framework for an agreement on implementation mechanisms for UN Security Council resolution 2216, a ceasefire and the restoration of a peaceful political transition." However, Hadi later [pulled out of the talks](#), as he conditioned his participation on Houthi agreement to accept the UN resolution. As no major political breakthrough has occurred, the Houthis have maintained their grip on power. In October 2015 they mobilized tribes loyal to them to stand united against activities perceived hostile to the Houthis. An [agreement](#) (in Arabic) signed by tribesmen and published by the government news agency (Saba News) under the control of Houthis said the tribes declared "freedom of liability," a term used to describe the tribal tradition that should someone hurt or even kill someone else for hostile activity, the offender would not be held responsible. The statement added that the "wrongdoers" should be punished according to tribal traditions, even if a political settlement is reached.

The United Nations High Commissioner for Human Rights released a [report](#) in September 2015 detailing the impact of the violence in Yemen, with over 1500 civilian casualties and widespread violations of international human rights law and humanitarian law. Saudi Arabia, however, has [resisted](#) calls by the United Nations Human Rights Council "for an international inquiry into abuses by all parties to the Yemeni conflict." In October 2015, the Netherlands [withdrew](#) a draft resolution that it, along with other Western countries, had sponsored that would have requested the United Nations High Commissioner for Human Rights to "send experts to Yemen to investigate the conduct of the war." Reacting to the collapse to establish an independent, international investigation into the conflict, Amnesty International, which headed the organization's fact-finding mission to Yemen, [stated](#), "The world's indifference to the suffering of Yemeni civilians in this conflict is shocking. The failure of the UN Human Rights Council last week to establish an international investigation into violations committed by all sides is the latest in a series of failures by the

international community to address total impunity for perpetrators of serious violations in Yemen.” Based on a [report](#) published in October 2015, Amnesty International stated: “Damning evidence of war crimes by the Saudi Arabia-led coalition, which is armed by states including the USA, highlights the urgent need for independent, effective investigation of violations in Yemen and for the suspension of transfers of certain arms.”

## Internet Infrastructure and Market in Yemen

Yemen has a small but rapidly growing population of Internet users. In 2014 the [International Telecommunications Union \(ITU\) estimated](#) that 22.55% of Yemeni citizens used the Internet, up from less than 1% a decade earlier and that the country has 340,000 fixed-broadband subscriptions, which works out to 1.36 subscriptions per 100 inhabitants. In March 2014, PTC [estimated](#) (in Arabic) the number of Internet users in Yemen to be 3,240,109 and the number of Internet cafes as 12,008. Mobile use has increased quickly in the last several years, with [ITU statistics estimating](#) the number of cellular subscriptions in the country in 2014 at just over 17 million.

Yemen is primarily served by one Internet service provider, the state-run YemenNet, which [dominates](#) the market amid calls from users to end the government monopoly over the Internet industry. YemenNet is part of the state-owned [Public Telecommunication Corporation](#), (PTC), which operates under the supervision of the Ministry of Communications and Information Technology. TeleYemen, another state-owned telecommunication provider, also provides Internet services, but its share of the market is not known. Yemen’s National Security Agency uses Internet filtering software to block political and pornographic content, which slows down Internet speeds [according to an official at YemenNet](#) quoted by local media. Yemen’s National Security Agency was [established](#) (in Arabic) in August 2002 by a presidential decree issued by then president Ali Abdullah Saleh, which established that its objectives are: to gather and make available intelligence related to Yemen's national security, to reveal and combat activities that sabotage Yemen's security, and to secure Yemen's borders and prevent penetration of foreign elements.

Figure 1 shows the centrality of YemenNet to the country’s international connectivity.

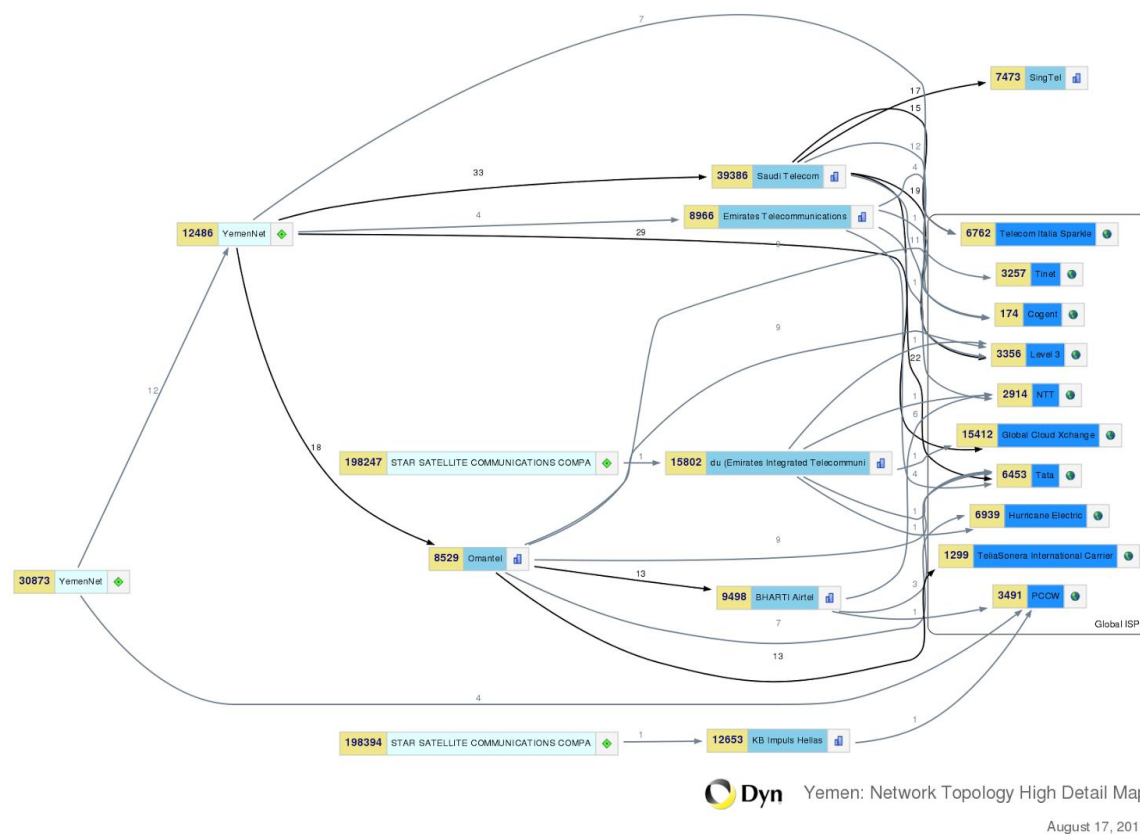


Figure 1: Map of YemenNet's international connectivity. (Image courtesy [Dyn](#))

## Pre-conflict Internet Filtering in Yemen

Prior to the conflict, Yemen had a long track record of filtering political content. The [OpenNet Initiative](#) (ONI) documented Internet filtering in the country dating back to 2006. Network measurement results from [2006](#) showed filtering of content from a variety of content categories, including pornography, anonymization tools, LGBT issues, and a small number of opposition political groups. Results from [2009](#) showed an increase in political filtering, including websites of opposition political groups and independent media. Interestingly, while filtering of some types of content (like pornography) was implemented with a descriptive blockpage noting the reason the content was blocked, political content was blocked using [injected TCP reset packets](#), a non-transparent method meant to emulate network connectivity problems. [This covert blocking](#) of political content provides plausible deniability to the government that is censoring constitutionally protected speech, while other types of content, like pornography, are blocked openly based on Sharia law. Internet censorship

during this period was performed with filtering products produced by the U.S.-based company Websense. However, following the ONI's publication of its reports, the [company blocked access to software updates from Yemen](#). Later ONI research showed that the ISP YemenNet had [switched to the products of Canada-based Netsweeper](#) to implement filtering.

## Part 1: Information Controls in Yemen in 2015

---

The following sections elaborate on several different forms of information control in Yemen during the 2015 conflict. We review the impact of the attacks on national electricity grids and the information environment in Yemen and how the scarcity of fuel and manipulation of its sale in a black market contributed to limiting alternative power generating methods needed to keep information infrastructure operational. We examine traffic data to Google services from Yemen against reports of power outages in the country, and use reports from the Internet performance monitoring company, Dyn, showing Internet outages. We then assess how these disruptions serve the interests of the parties involved in the political and armed conflict. We also review attacks on media professionals and outlets, reports of expanded Internet filtering, politically motivated breaching of websites, digital surveillance, and removal of TV channels from satellite operators.

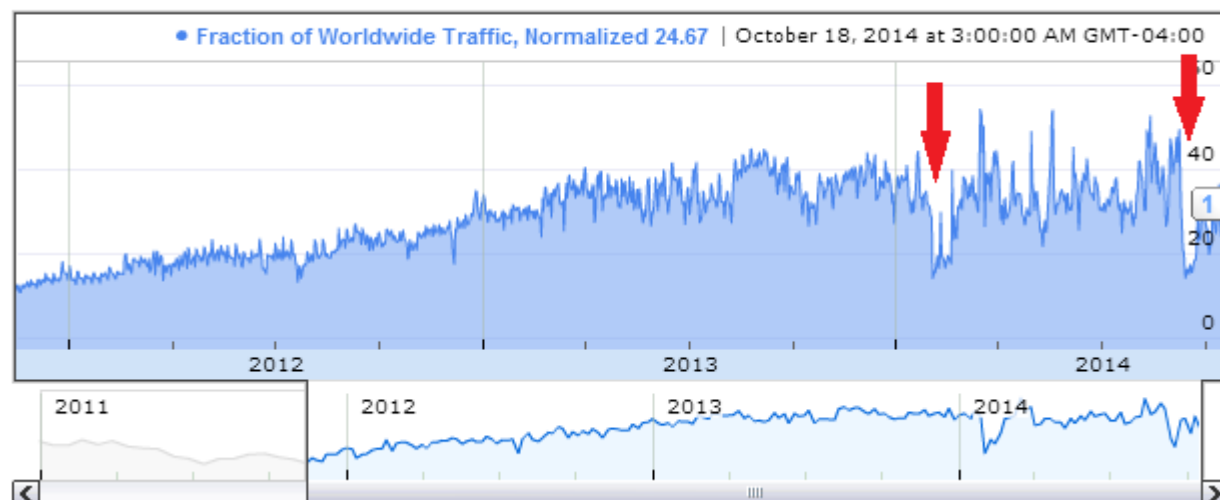
### Electricity and information control



*Figure 2: Fuel truck unloads and sells gas in the streets of the Houthi-controlled capital city of Sana'a, instead of gas stations where it can be sold at official price. (Photo credit: Naser Noor)*

Information and communication technologies require electrical power for operation, and so access to electricity is a fundamental element of information control. Frequent attacks on national electricity grids have disrupted access to telecommunication and Internet services. Google real-time data of traffic to its products and services shows a sharp drop in traffic on certain dates. We examined these dates against media reports on attacks on electricity grids and found a correlation. Figure 3 shows sharp drops occurring occasionally, such as on the week of February 3 and the week of September 12, 2014. [Media articles](#) report attacks on electricity system on these weeks.

### Fraction of Worldwide Traffic, Normalized



*Figure 3: Traffic data to Google services from Yemen, showing frequent disruptions during 2014. [Source]*

As the armed conflict intensified, access to electricity has been heavily disrupted. National [electrical lines were destroyed](#) in June 2014 as a result of violence in the governorate of Marib, which houses the country's primary power plant. Engineers from the Ministry of Electricity and Power were [unable to repair the damaged grid lines in the active conflict zone](#) amid conflicting accusations of who is responsible for disobeying a ceasefire. Similarly, much of the country was left without electricity on April 13, 2015 following an [attack on power transmission lines](#).

The electrical shutdown combined with the severe shortage of fuel needed to operate household generators (for those who can afford them) has resulted in citizens without access to television or the ability to power computers or mobile phones. The *Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General* stated that Saudi-led coalition [caused fuel scarcity in the local market](#), saying: “Severe import restrictions, caused mainly by the naval blockade imposed by the coalition forces during the conflict, have also aggravated the humanitarian situation, resulting in fuel scarcity, which adversely affects the distribution of food and water, as well as the functionality of hospitals.”



*Figure 4: Long line of taxis waiting for gas to be available at a gas station in the city of Sana'a. (Photo credit: Naser Noor)*

Moreover, local media has [reported](#) (in Arabic) that the Houthis have created and operated a black market for fuel so that they can sell it at a much higher price to finance their military operations. The reports [publish](#) photos of what they describe as gas trucks unloading and selling in the streets instead of delivering the fuel to gas stations where it can be sold at the official price (see also Figure 2 above). The lack of easy access to fuel has also brought about scarcity in access to information. Without fuel to power generators, and thus electrical powered computers and television, [battery-operated radios](#) have become the primary source of information. Notably, the only local radio news stations available are Sana'a Radio Station, which is government-operated, and al-Masirah, the official Houthi radio station. Like many government media

institutions, the Sana'a Radio Station is controlled by the Houthis since they took control of the capital city of Sana'a. As a result, the editorial policy of government radio reflects Houthis' political points of view, and the station is essentially a mirror of al-Houthi's official radio, al-Masirah. Therefore, Yemenis are left with news and views [reflecting a single political opinion](#).

Moreover, the significantly degraded telecommunication services and unavailability of fuel have had a direct detrimental impact on the lives of civilians living in active military operations. *The Annual Report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General* [notes](#) that in May 2015 the Saudi-led coalition forces declared a military operation against the Houthis stronghold governorate, Sa'ada, and warned civilians to stay away from what they said were Houthi locations and crowds. The forces declared the cities of Marran and Sa'ada military zones. The report states that "[a]ccording to Saudi State television channel Al-Ekhbariya, flyers announcing the operation were released over Old Sa'ada", however "the limited availability of fuel, the particularly challenging terrain, and barely operational telecommunications services prevented tens of thousands of civilians from complying with the ultimatum launched by the coalition." The same report says OHCHR later observed that coalition air strikes hit at least six residential homes and five markets, but it was not able to obtain detailed information on resulting casualties.

The electricity outage and shortages in fuel have affected other forms of media as well. A number of [newspapers have ceased to publish](#) due to the lack of power, and some websites, such as the news portal News Live, [announced](#) (in Arabic) they are no longer able to publish as the telecommunication disruption has left them unable to receive updates.

As disruptions to electricity can be caused by violence or deliberate manipulation, they are often accompanied by mutual accusations of responsibility. Power outages can also have coincidental impacts that benefit some groups over others. Although we cannot determine which side of the armed conflict is responsible for all the disruptions, power outages as a whole appear on balance to favour the Houthis and their strategy of degrading information flows. Accusations that they are manipulating fuel supplies as part of a broader information control strategy warrants further research, a topic to which we return again in the next section.



*Figure 5: A busy street in Sana'a in total darkness because of electricity shutdown, except for the lights of the cars. (Photo credit: Naser Noor)*



*Figure 6: Businesses rely on gas-operated power generators like this one outside a shop. (Photo credit: Naser Noor)*

## Internet and telecom disruptions

Similar to disruptions during the [2011 revolution in Egypt](#) or the [ongoing Syrian conflict](#), international telecommunications connectivity in Yemen has been either completely or partially disrupted several times during the armed conflict. The number of routing instabilities has increased since the conflict escalated in late March 2015, as shown in Figure 7:

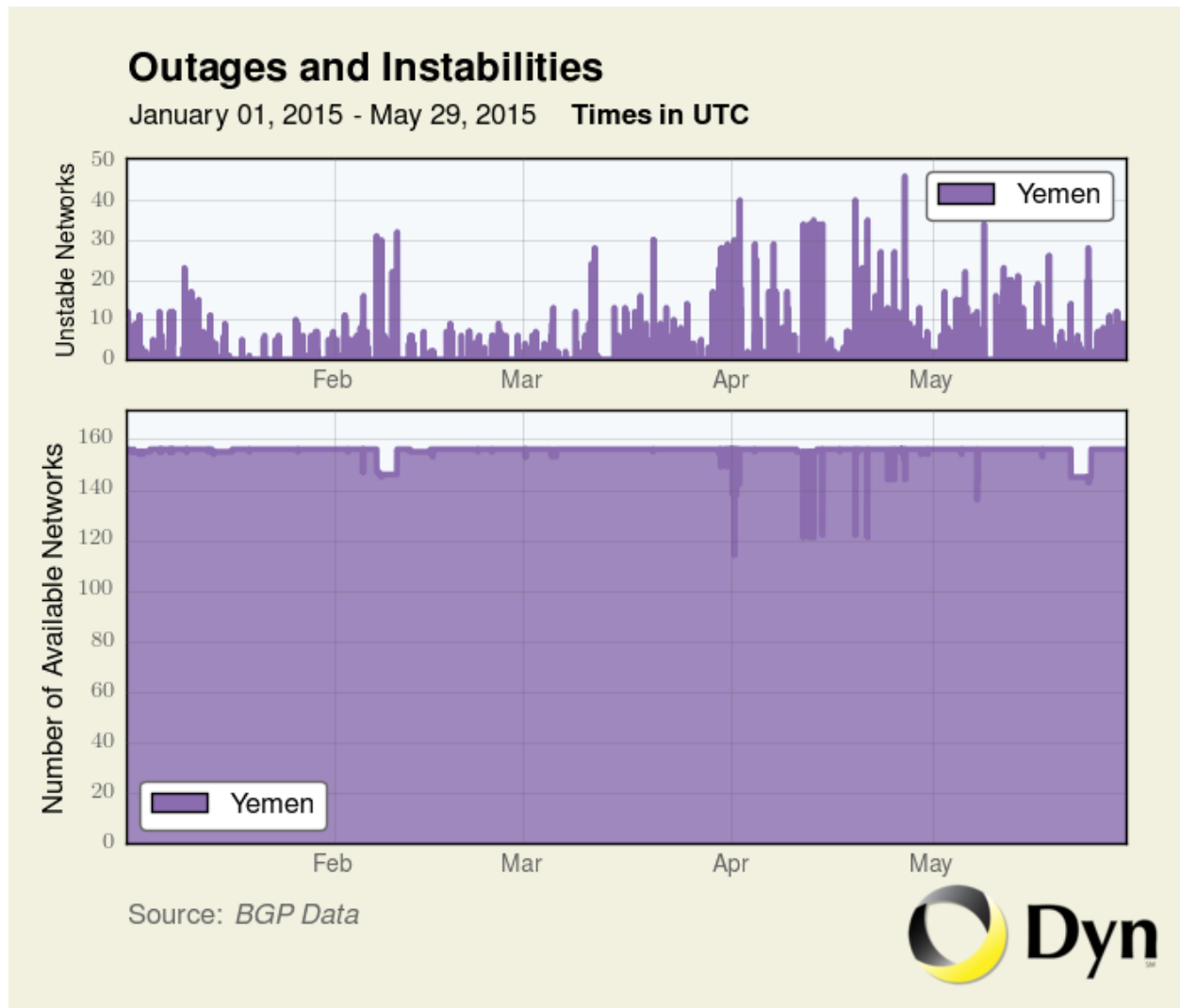


Figure 7: Traffic data showing increase in unstable networks and unavailable networks in Yemen. (Image courtesy [Dyn](#))

On March 31, 2015, [international telecommunications services to and from Yemen were cut off](#) briefly by the Houthi-controlled Ministry of Communications and Information Technology. At the end of March and in early

April 2015, [another outage occurred](#) affecting Yemen's submarine fiber connection to neighbouring Djibouti (See Figure 8) -- particularly problematic as Yemen has only two international submarine fiber connections.

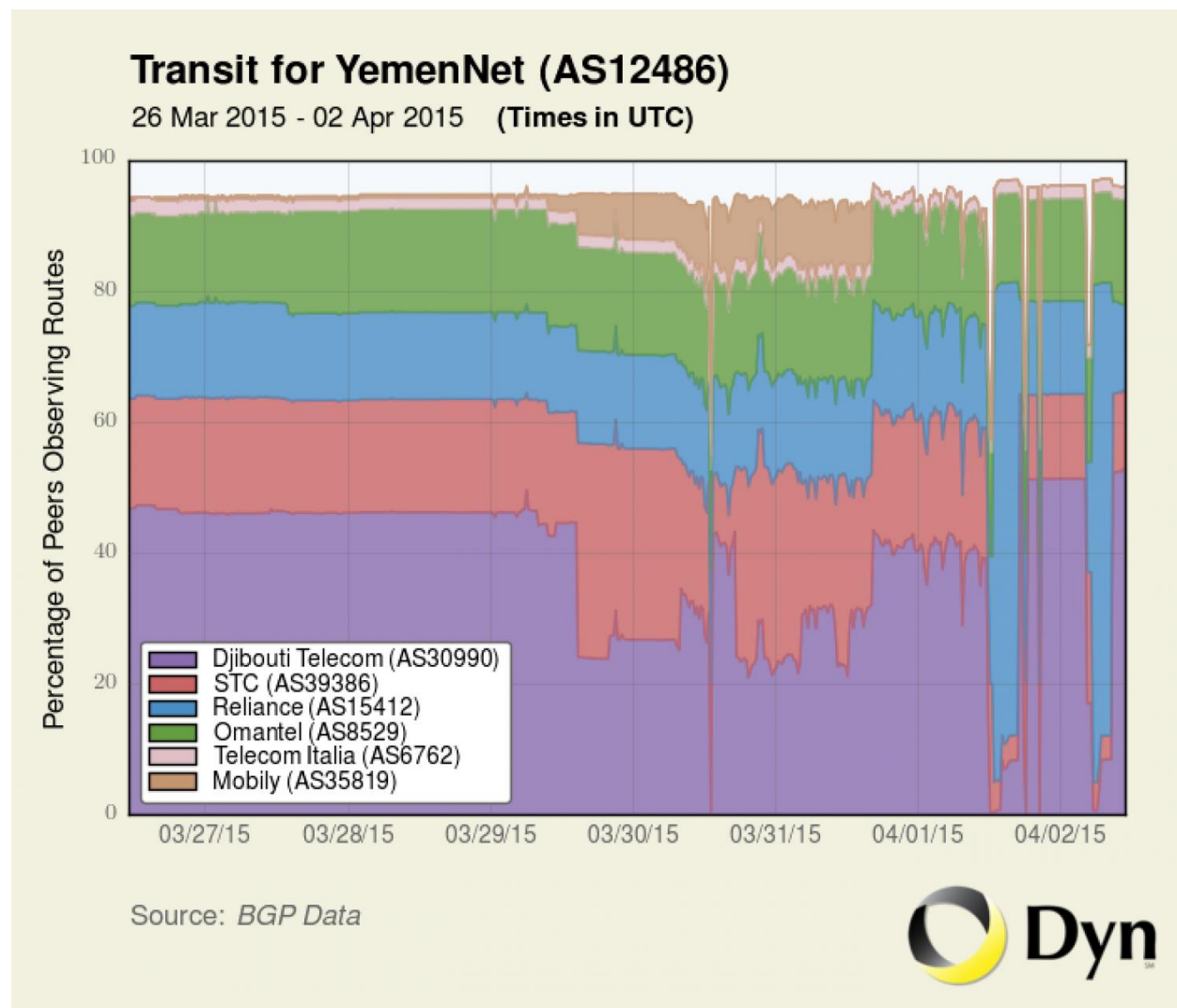
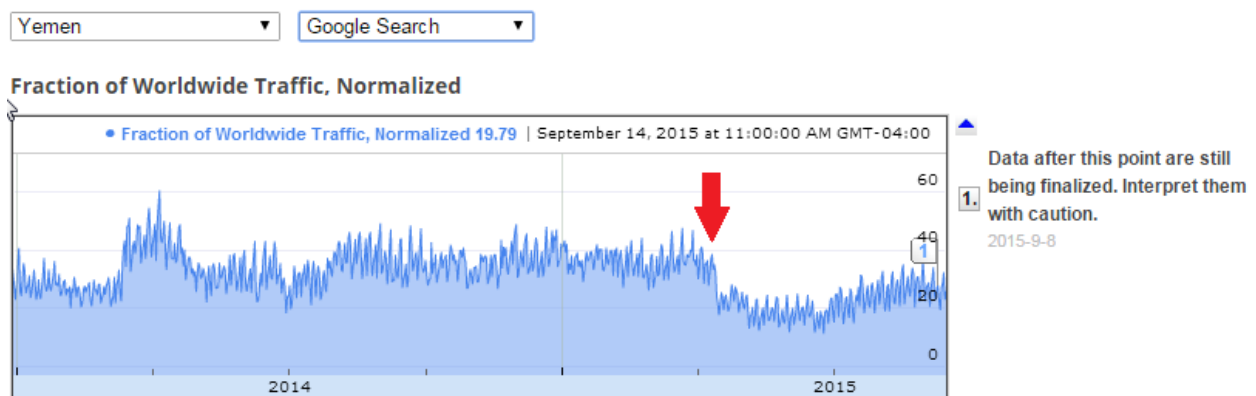


Figure 8: Traffic data from YemenNet showing impact of disrupted submarine fiber cable. Source: [Dyn](#)

Reports emerged on April 7, 2015 that the Ministry of Communications and Information Technology had [cut off phone and Internet connections in the city of Aden](#) following fighting between supporters of president Hadi and Houthi rebels. On April 12, Internet connectivity was disrupted in numerous cities throughout the country. [Conflicting reports from local media](#) attributed this disruption to a severed international fibre optic cable, while others suggested the disruption was a result of the installation of filtering and surveillance equipment on the national network by the Ministry of Communications and Information Technology.

In late April and early May 2015, telecommunications systems were at risk of going offline as a result of fuel shortages throughout the country. On April 28, [local media reported](#) that Houthi rebels had seized gasoline and diesel shipments intended for humanitarian relief, including shipments intended for telecommunications providers, who had been relying on generators as a result of instability in electrical infrastructure. As a result, the Ministry of Communications and Information Technology announced that it would sever Internet access in four governorates (Aden, Dhale, Abyan and Lahj) on May 1 as a result of the fuel shortages. Days later, local media [reported](#) that the Ministry of Communications and Information Technology announced that this shutdown would extend to the entire country, beginning on May 4 at 9:00am. However, the Ministry later [announced](#) that they had secured the required fuel to maintain telecommunications service and a shutdown was avoided.

Other data sources have illustrated the impacts of disrupted Internet traffic and widespread power outages. Figure 9 shows traffic from Yemen to Google's search services, with the red arrow showing the steep drop-off in traffic on April 13, 2015, the date of a [major power outage](#) in the country.



*Figure 9: Traffic data from Yemen to Google Search services showing significant disruption beginning in mid-April 2015.*

Beginning May 30, 2015 there was a further disruption on YemenNet affecting its upstream link to upstream provider Reliance, as shown in Figure 10:

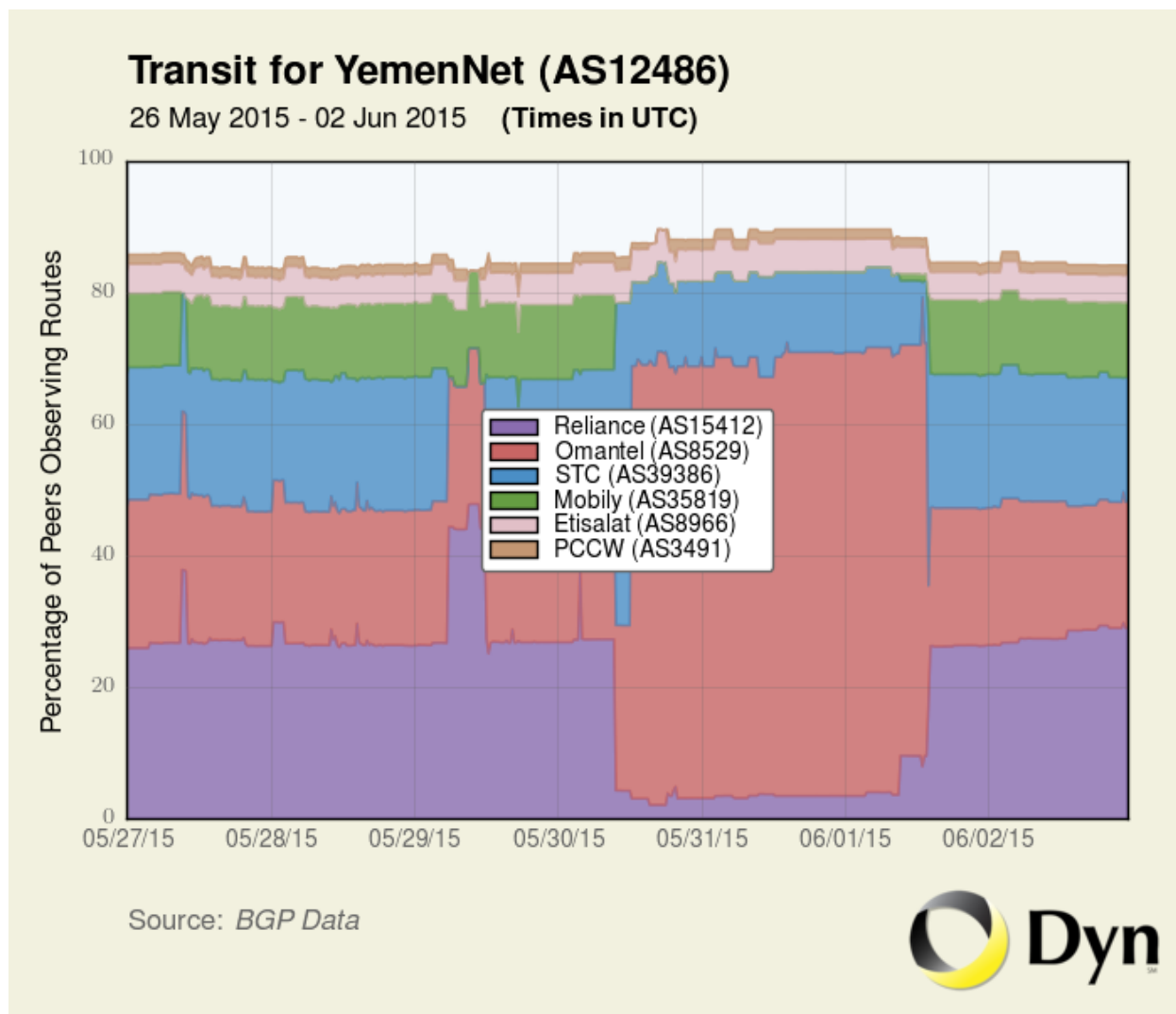


Figure 10: Traffic data showing May 30 disruption between the ISP YemenNet and upstream connection Reliance. (Image courtesy [Dyn](#))

Conflicting reports emerged about the cause of this disruption. The Houthi-controlled Ministry of Communications and Information Technology claimed the disruption was the result of [damage to fibre optic cables](#) in a number of locations. Local media sources disputed this account, instead attributing the outage to [increased filtering by the Houthi-controlled Ministry](#), citing individuals who used circumvention software to access sites which were otherwise inaccessible -- an act which would not be possible if the disruption was caused by fibre optic cable damage.

## Internet filtering

Following the 2015 Houthi takeover of power, the scope of filtered content in Yemen has increased. [Reports](#) emerged that the Ministry of Communications and Information Technology, under the control of the Houthis, began blocking additional independent news websites including Mareb Press, Yemen Voice, Sahafa Net, Al-Sahwa Net, and Yemen Press. This increase in blocking [was condemned](#) by the Yemen chapter of the Internet Society.

In June 2015, in response to the increase in political filtering, a number of Yemeni websites and journalists [established](#) (in Arabic) the Electronic Media League to Fight Website Blocking. The League agreed to collectively adopt a new editorial policy, including the use of specific terminology to describe the Houthis. For example, they agreed to refer to Houthi leader Abdulmalik Al-Houthis as the “rebel,” and the Houthi movement as the “rebel movement” and the “rebel Houthi militia.” The league promised further media escalation and criticized the Houthi movement for trying to enforce an information blackout and create tensions with the media.

There have also been reports of an increase in Internet filtering on the other side of the military conflict, in Saudi Arabia. On April 28, local media [reported](#) that the Saudi authorities blocked Yemeni government news websites controlled by the Houthi rebels and websites affiliated with ousted president Saleh, an ally of the Houthis. Other [media reports](#) said Saudi authorities are censoring clerics who criticize the Kingdom's military intervention in Yemen.

We provide a detailed analysis of our own testing of Internet content filtering in Yemen, Saudi Arabia and Iran in Part 2 of this report.

## Targeting journalists and media outlets

After seizing power in September 2014, Houthi forces targeted media outlets and journalists through raids, kidnapping and harassment. Reports emerged that [gunmen raided at least four news outlets](#), detaining staff and confiscating equipment. [Other reports](#) have said the Houthis continue to target journalists, media outlets and media support institutions by means of death threats, abduction and looting, with at least 67 cases of such methods (as of March 2015) used to stop journalists from doing their work.

Another report [says](#) Yemeni journalists face their “toughest times ever” as a result of the Houthi militia’s violations of press freedoms, which have included kidnapping, detention and physical aggression, beatings, and forced disappearance of journalists working for local and international media outlets. The report adds

that these violations, as well as an economic recession and the shortage of fuel, have forced many local independent media to stop printing and cease operating their online presences, leaving the market solely with media owned by the Houthis and Saleh, whose control over government financial institutions allows them to finance such media using public money.

In April 2015, the Houthis [launched an investigation](#) into 39 politicians, activists, and journalists for allegedly compromising “the country's independence, unity and territorial integrity.” The figures include Yemen’s Nobel Peace Prize laureate Tawakkol Karman and reporters of local TV stations. Also in April 2015, Yemeni journalist [Waheed al-Sufi was reported to have been kidnapped](#) by armed gunmen, and his current whereabouts are unknown.

Activists [accuse](#) the rebels of intentionally imprisoning their opponents in military sites known to be coalition targets. On May 20, [two Yemeni TV journalists were abducted](#) by militiamen allegedly aligned with the Houthis. Also in May, [local](#) and [regional](#) media reported that Houthis used kidnapped journalists as [human shields](#) at military locations, and as a result two journalists were killed in airstrikes. In August 2015, it was reported that [11 journalists remain held hostage](#) by the Houthis, 9 of which were abducted simultaneously in Sanaa in June.

After having its [offices raided and its website blocked](#), news website Almasdar Online moved its operations outside of Yemen. Mobile phone operators reported that they have received orders from the Houthi rebels to [stop the news alert services](#) sent by media organizations to mobile phones.

In March 2015, the Houthi rebels [raided and shut down](#) local TV channels including Suhail TV, Yemen Youth TV, Al-Saeedah TV, Maeen TV and the office of the pan Arab Aljazeera TV.

The Houthis have also shut down radio stations. In September 2014, they [raided](#) (in Arabic) the headquarters of local social radio station Hayat FM and confiscated its equipment. The equipment was returned to the radio station after negotiations with the Houthis, but the Houthis raided and shut down the station again in June 2015. The station remains shut down as of the writing of this report.

Because the government of President Hadi lost control over government news websites, including the official state news agency Saba News, it [launched a new Saba News website](#) in May 2015 with the same design but a slightly different domain name (<http://sabanew.net/> as an alternative for <http://sabanews.net/>). The website was to represent the “legitimate” government and act as an alternative to the original Saba website that has been under the control of Houthi rebels. The Houthi-controlled Saba news agency later [issued a statement](#) describing the new website as fake and a moral and intellectual crime. In an attempt to reach out to citizens

inside Yemen, the Saba News website, which is run by the internationally recognized government [launched](#) (in Arabic) in August 2015 a news update service via the application WhatsApp. It asked users to subscribe to the service by adding the Egypt-based phone number 00201151665166. It also launched a news update [application](#) for Android mobile devices.



*Figure 11: Screenshot from Yemeni private TV channel Azaal TV. Arabic banner says: “The terrorist Houthi militia continues to occupy Azaal TV station headquarters in Sana'a after it raided it, confiscated its equipment, and expelled its staff.” (Photo credit: Naser Noor)*

In September 2015, the Yemeni coalition for monitoring human rights violations [discussed](#) (in Arabic) at the Office of Human Rights Commission in Geneva what it called the “documented atrocities of the Houthi and Saleh militias” committed between September 21, 2014 and August 15, 2015. The coalition documented offenses including the Houthi confiscation of most government-own media outlets and their controlling of the Ministry of Communications and Information Technology and the national ISP YemenNet, “which enabled it to block 61 websites.”

Saudi-led coalition forces have been accused of targeting Yemeni media outlets. In April 2015 for example, a blast caused by a coalition airstrike in Sana'a [killed a TV journalist and three staff members of the Satellite TV station Yemen Today](#), which is affiliated with ex-president Saleh. The manager of the TV station accused the coalition of targeting the media outlet because Saleh is an ally of the Houthis. A few weeks earlier, the

collation spokesperson had said that media outlets supporting the Houthi rebels would be targeted, but he did not explain how. An email request for explanation from the Committee to Protect Journalists that was sent to the Saudi Embassy in Washington was not answered.

## Contestation over TV broadcasts

Yemeni TV channels operated by the competing political and armed parties have been the focus of contestation. While Houthis used their military power to raid, physically control, and editorially shape the state-run TV stations, the government of president Hadi used its political influence to have these channels taken off air by the regional satellite providers covering the Middle East and North Africa. State-run television channel Aden TV, which prior to the Houthi takeover had been under the control of the government of President Hadi, has been the object of intense contestation. In February 2015 the Houthis hijacked the broadcast frequencies of the channel, forcing the channel [to resume broadcasting](#) on new frequencies. Further back-and-forth [hijacking attempts](#) continued in March.

The contestation continued at another level. In March, the two primary regional satellite broadcasters, Egypt-based Nilesat and Saudi-based Arabsat, [stopped broadcasts of Yemeni state-run channels](#) at the request of President Hadi after the channels fell under Houthi control. In May, Nilesat [dropped the Houthi-owned channel Al-Masirah](#), knocking it off the air for millions of subscribers in the Middle East and North Africa. The channel would later advertise new frequencies on a Russian satellite. Also in May, Nilesat [stopped broadcasting Yemeni TV channel Yemen Today](#), which is owned by toppled president Saleh. Saleh has been [targeted](#) by the Saudi-led coalition for backing the Houthi rebels; on May 10 his house in Sana'a was destroyed by airstrikes. There have been no statements from either Nilesat or Arabsat as to which specific party requested the TV channels be dropped, nor have there been any official statements about the legal frameworks used to take such a measure by either of the satellite providers. We sent queries to the broadcasters ([Nilesat](#) and [Arabsat](#)) seeking an explanation on October 15, 2015, but as of the time of publication have not received a reply.

## Electronic surveillance

Foreign and domestic electronic surveillance is widespread in Yemen, existing prior to as well as during the current armed conflict. Political rivals have allegedly conducted surveillance on their political enemies throughout the ongoing armed conflict. For example, amidst the political rift between the Houthis and President Hadi in January 2015, the Houthis [broadcast](#) (in Arabic) on their TV station al-Masirah a telephone

conversation between Hadi and his office manager discussing political issues that the Houthis criticized. In the same month, al-Jazeera [broadcast](#) a leaked telephone conversation allegedly between ex-president Saleh and a Houthi leader "apparently coordinating military and political moves." The government of President Hadi has [accused](#) Iran of operating spy cells in Yemen that include members of the Iranian Revolutionary Guard, for the purpose of aiding the Houthis. The Minister of Interior in the government of President Hadi [said](#) (in Arabic) Iranian-made advanced surveillance and wiretapping equipment was found in Aden in July 2015 after fighters loyal to the government of president Hadi regained control of the area.

The Saudi airstrikes have been in part [guided by intelligence from aerial surveillance performed by the United States](#), with American military planners "using live intelligence feeds from surveillance flights over Yemen to help Saudi Arabia decide what and where to bomb," while also [monitoring the Saudi-Yemen border](#) for potential security threats. Such intelligence sharing is a continuation of a long-standing American surveillance program aimed at [identifying and locating members of AQAP](#). This program has included the use of predator surveillance drones and "sophisticated surveillance and electronic eavesdropping systems operated by spy services including the National Security Agency."

Since seizing power, the Houthi rebels have also allegedly sought to conduct surveillance activities. Aden Telecom General Manager Abdulbasit Al-Faqih [accused the Houthi rebels](#) of wiretapping telecommunications in the country. In an interview with local media, he claimed that Houthi rebels actively wiretap communications in Yemen, and that the country's national security agency in Sana'a, which is under the control of the Houthis, possesses surveillance equipment. The official [told the media](#) that "the Houthis now wiretap all of our communications, and they can wiretap my telephone call with you now." He added that the equipment provided by Washington to conduct counterterrorism in Yemen is now being used by the Houthis, adding that telecom offices in Aden do not have the capacity to wiretap communications and as a result the activities of the rebels cannot be tracked. The official claimed that Houthi rebels, especially their key leaders, [use Thuraya equipment for communications](#), which implies that they have an alternative communication system.

Social media posts have also suggested that the mobile phones of killed or captured anti-Houthi fighters were examined to identify contacts and conversations, particularly messages shared over the [messaging application Whatsapp](#).

On May 31, 2015, a local news website [quoted](#) (in Arabic) an unnamed source at Yemen Mobile, a mobile phone provider in Yemen, as saying that the Houthis and allies of ousted president Saleh are using the mobile network to monitor calls and text messages, as well as to perform round-the-clock surveillance on the

location of their opponents to determine their movements in armed conflict zones. The company [denied](#) the allegations in a statement, saying it respects the privacy of its users according to the law, and that Houthis do not interfere in the company's affairs. Another mobile company, Y GSM, [issued](#) a statement denying similar accusations that appeared in the local media. We cannot independently verify these claims at this time.

Email messages leaked from the spyware firm Hacking Team show that multiple requests were made from companies in Yemen seeking assistance deploying surveillance tools in the country. In May 2013 an individual from an [IT contractor in Yemen contacted Hacking Team](#), stating they they were a customer of the Yemeni National Security Agency and were looking for more information on Hacking Team's Da Vinci interception system. Similarly, in March 2015 a separate IT contractor in Yemen [contacted the company](#) requesting assistance, claiming to be the CEO of an IT security company who had a contract with Yemen's NSA to "develop systems, training & set up of a powerful tool to monitor, intervene, analyze, locate & control the total Telecom spectrum of the Republic of Yemen." It is not clear from the leaked email threads whether either of the companies procured Hacking Team's products or services. None of the scans we have undertaken as part of Citizen Lab research on Hacking Team and Finfisher so far have shown evidence of Yemen-based control servers.

## Targeted digital attacks

Targeted digital attacks have become a regular feature of conflict in recent years, particularly in the Middle East and North Africa. The Syrian Electronic Army has [targeted websites for defacement](#) in order to [spread pro-regime messages](#) since 2011. Similarly, a group known as the Yemen Cyber Army has emerged to take credit for a number of notable compromises.

In April 2015, individuals identifying themselves as the Yemen Cyber Army [compromised the website of pan-Arab newspaper al-Hayat](#), displaying a photo of Hezbollah leader Hassan Nasrallah as well as slogans used by the Houthis. On May 22, 2015, as the Saudi-led airstrikes in Yemen continued, the Yemen Cyber Army claimed responsibility for compromising computer networks of the Saudi government Ministries of Foreign Affairs, Interior, and Defense, and leaking what it called top secret documents revealing spies' identities, according to Russian news agency [Russia Today](#). An official from the Saudi Ministry of Foreign Affairs [acknowledged](#) the compromise in a statement released by the government official press agency. The official said the computer networks at the Ministry of Foreign Affairs were targeted and that an investigation had been launched in coordination with other concerned authorities in the Kingdom. The official warned that the compromise should not be exploited to produce and disseminate fake documents, adding that disseminating such documents helps the "enemies" of the Kingdom, and is criminalized by the Kingdom's Anti-Cyber Crime

Law. Iran's Fars News Agency reported on the compromise and [included links](#) to the alleged leaked documents. Iran's Press TV also [ran](#) a report on the incident.

In July 2015, the Yemen Cyber Army [reportedly released a list of 23 websites](#) of Saudi companies which were to be targeted for attack, although there has been no evidence that any of the websites have been affected. However the group's alleged links to Yemen have been contested. Multiple security experts have suggested, based on the [infrastructure used to distribute compromised data](#) and the [malware used to conduct the Saudi Ministry of Foreign Affairs](#) compromise, that the attackers [are more likely Iranian](#) and may be sponsored by the Iranian government.

In September 2015 the website of the Indian Bureau of Energy Efficiency was compromised and defaced with a messaging [attributing the defacement to the "Yemeni Electronic Army"](#).

## Part 2: Network Measurement Results

---

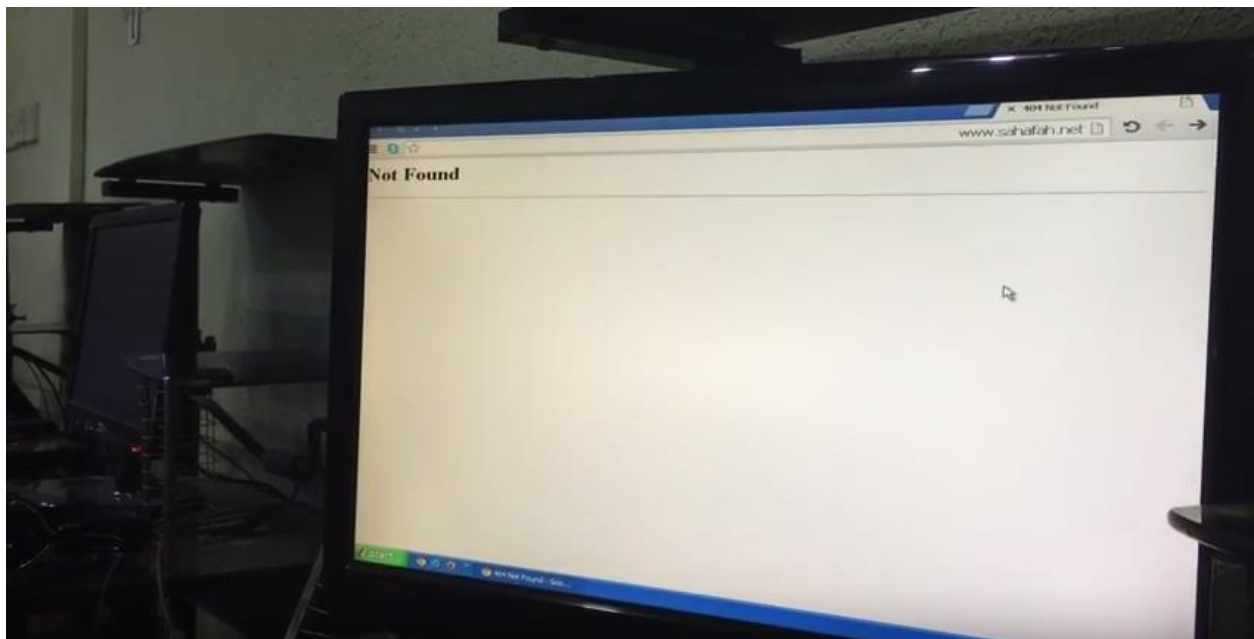
This section examines the results of our tests for filtering of web content in Yemen, Saudi Arabia, and Iran in the context of the political and armed conflict in Yemen. The three countries, as already described, were significant censors of web content before the conflict began and reports have emerged suggesting that censorship has expanded in each of the countries as the conflict escalated. Network measurements in Saudi Arabia and Iran show the degree to which the conflict has been internationalized, with contests over information controls extending beyond Yemen's borders and impacting each country's censorship practices.

We ran network measurement tests to determine what content was censored, how censorship was applied, whether the censorship was transparent or not, and if the technology used to implement web censorship could be identified. In addition, knowing that censorship in Yemen has [previously been implemented with technology from Canada-based Netsweeper](#), we sought to determine if a Netsweeper installation was still active in Yemen, and if so whether it was communicating with or otherwise receiving updates from Netsweeper servers. Any provision of corporate services to YemenNet, a state-owned and operated national ISP that is now controlled by the Houthi rebels, raises a number of questions regarding corporate social responsibility and complicity in information controls tied to armed conflict (which we address later in the report).

Part of the research for this report, including a portion of the network measurement tests, was undertaken by an independent researcher in collaboration with the Citizen Lab from within Yemen. The researcher happened to be stranded in the country during part of the armed conflict period, and was not requested by Citizen Lab to travel to Yemen for research purposes. Network measurements run with the ICLAB platform are conducted under a research protocol that has been reviewed and approved by the University of Toronto's Research Ethics Board. That protocol explicitly restricts undertaking research in high risk environments, including zones of conflict, and in previous work we have avoided running measurements in such environments. However, gauging risks is always difficult as the situation on the ground is fluid and dynamic, and can change quickly. The independent researcher was fully cognizant of these risks and gave free and informed consent to conduct the research. We maintained regular consultations about evaluating the level of risk involved in running tests and undertaking field research. Throughout this project, efforts were made to mitigate the risk as much as possible. Once the armed conflict in Yemen became particularly acute, we ceased all field research and network measurements.

#### a. Yemen

Soon after the conflict began, [reports emerged](#) that the Houthi-controlled Ministry of Communications and Information Technology in Yemen had added new websites to the list of censored websites in the country. In order to confirm these reports of increased filtering, we performed network measurement tests to identify the types of content filtered and the method of filtering.



*Figure 12: A user in Yemen receiving a “Not Found” error page when trying to access news portal sahafah.net (Photo credit: Naser Noor)*

From March to July 2015, we conducted network measurement tests on networks in Yemen. Measurements were conducted using the [ICLab](#) platform. These tests consisted of a software client performing an HTTP GET request for a predefined list of URLs, and collecting the responses. These responses were analyzed to identify instances of deliberate filtering.

The sample of URLs tested consisted of two lists. The first list was the list of [top 500 most popular websites](#) as determined by Alexa. The second list was specific to Yemen’s local political, social, and cultural context, including websites representing those who are believed to be aligned with the government of president Hadi; the Houthis, ex-president Ali Abdullah Saleh, and political parties; government media; partisan and nonpartisan media; independent news portals; NGOs and advocacy groups; discussion forums; and a collection of apolitical cultural and entertainment websites. In total, 793 URLs were tested in Yemen. The full list of tested URLs can be found in the Data section below.

In some cases, as reports emerged of new content being blocked, we added relevant URLs to the testing list. In addition, after initial test results showed that all URLs on our list using the Israel top-level domain (.il) were blocked, we included additional .il URLs to determine if all such URLs were blocked.

The testing lists are not comprehensive and do not attempt to identify every URL that may be blocked. Rather, they are a snapshot of potentially sensitive or reportedly blocked URLs covering a range of relevant content categories.

In addition, we [conducted network scans using the search engine Shodan](#) and other tools aimed at identifying instances of Netsweeper installations in Yemen.

Tests were performed on the ISP [YemenNet](#). Analysis of the data gathered on YemenNet showed a number of test results that we believe reflect deliberate attempts to filter content. This filtering took two forms: A descriptive Netsweeper blockpage and a ‘404 Not Found’ error page. The descriptive blockpage clearly indicated that the content was blocked, while the ‘404 Not Found’ page was designed to emulate a technical error. Thus, some content was openly blocked (transparent) while other types of content were blocked with a response designed to confuse users (non-transparent).

Netsweeper blockpage

The first form of filtering returned a series of similar blockpages like the one shown in Figure 13:

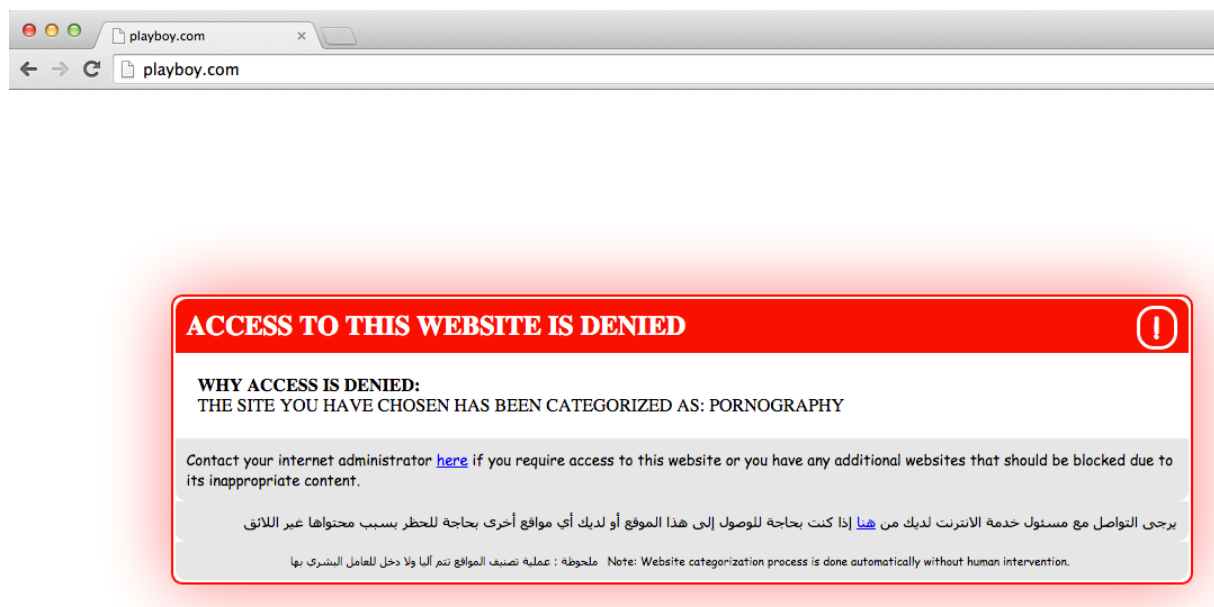


Figure 13: Descriptive Netsweeper blockpage for an attempt to access playboy.com

This blockpage transparently identified the content as blocked, the category of the content (in most cases), and provided a method for disputing this categorization. The HTML source of this blockpage looked as follows: (requesting IP address has been redacted)

```
<iframe
src="http://82.114.160.94/webadmin/deny/?dpid=5&dpruleid=3&cat=23&ttl=-200&groupname=default&policyname=default&username=-&userip=X.X.X.X&connectionip=127.0.0.1&nsphostname=NS-PS03&protocol=policyprocessor&dplanguage=-&url=http%3a%2f%2fplayboy%2ecom%2f" width="100%" height="100%"
frameborder=0></iframe>
```

This page source, in particular the string '/webadmin/deny', is [consistent with the use of Netsweeper](#) filtering products. In addition, an alternate version of the blockpage with the Netsweeper logo can be found hosted at the same IP address at <http://82.114.160.94/webadmin/deny/?dpid=2>, as shown in Figure 14:

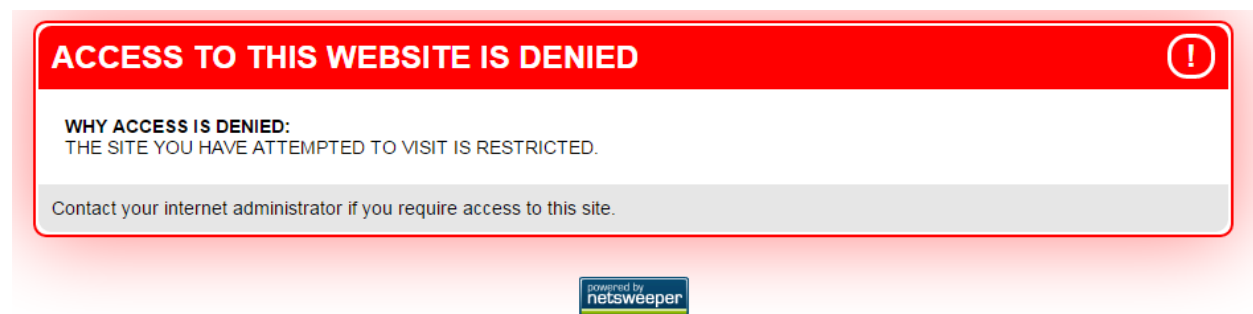


Figure 14: Alternate version of the blockpage containing the Netsweeper logo hosted on YemenNet.

There are a number of data points related to this Netsweeper installation that we can identify from this page source. First, we are able to determine the content category Netsweeper has assigned to a given URL from this blockpage text. Each content category is [given a unique number](#) by Netsweeper, including the custom category fields which may be created by systems administrators. For example, the text fragment "&cat=23" shown in the above HTML source indicates that this URL belongs to Netsweeper category number 23 ('Pornography'), which matches the description shown in the blockpage displayed in Figure 13. In total, we identified four blocked content categories: Pornography (23), Web Proxy (32), Nudity (3) and Custom (105). While the Pornography, Web Proxy, and Nudity categories are predefined by Netsweeper, the Custom category was likely created and maintained by system administrators at YemenNet.

Blocked URLs that belonged to the 'Web Proxy' category triggered the blockpage seen in Figure 15:

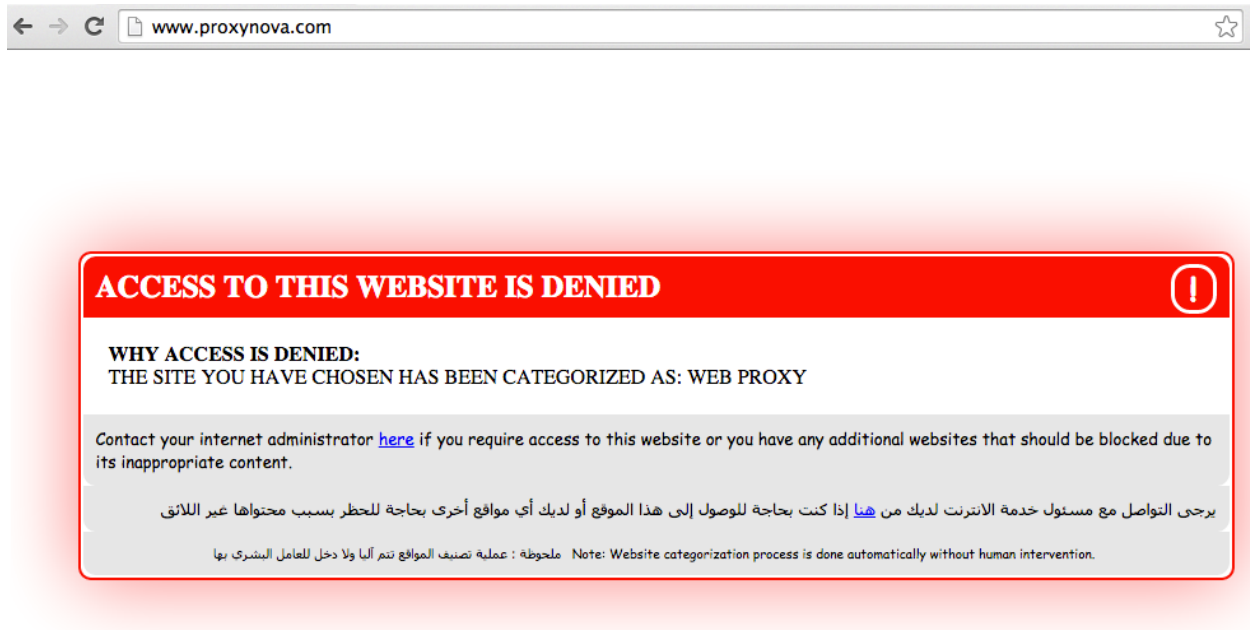


Figure 15: Blockpage displayed for URLs categorized as 'Web Proxy' by Netsweeper

For blocked URLs that belonged to the 'Nudity' category, the blockpage shown in Figure 16 was displayed:

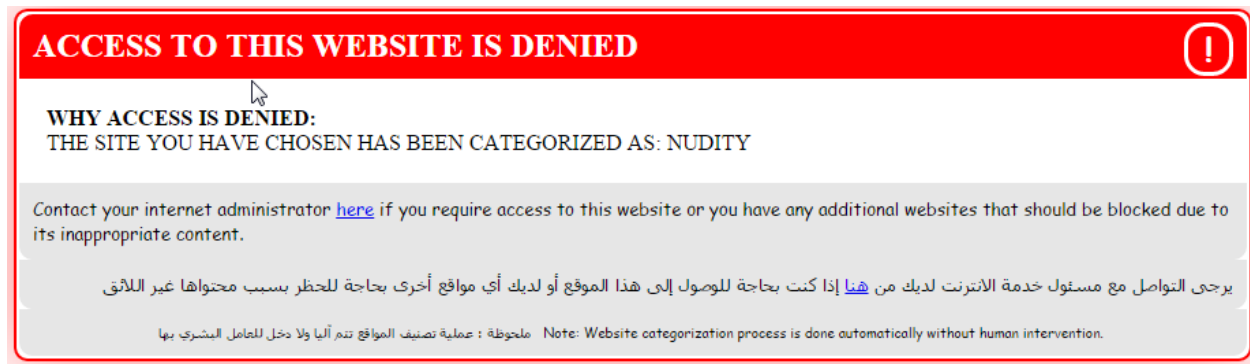


Figure 16: Blockpage displayed for URLs categorized as 'Nudity' by Netsweeper

For blocked URLs that belonged to the 'Custom' category, the blockpage containing the more generic text "Your administrator has blocked this site" as shown in Figure 17 was displayed:



Figure 17: Blockpage displayed for URLs belonging to the 'Custom' category

The breakdown of URLs found blocked in each category, as a percentage of total blockpages returned, is shown in Figure 18:

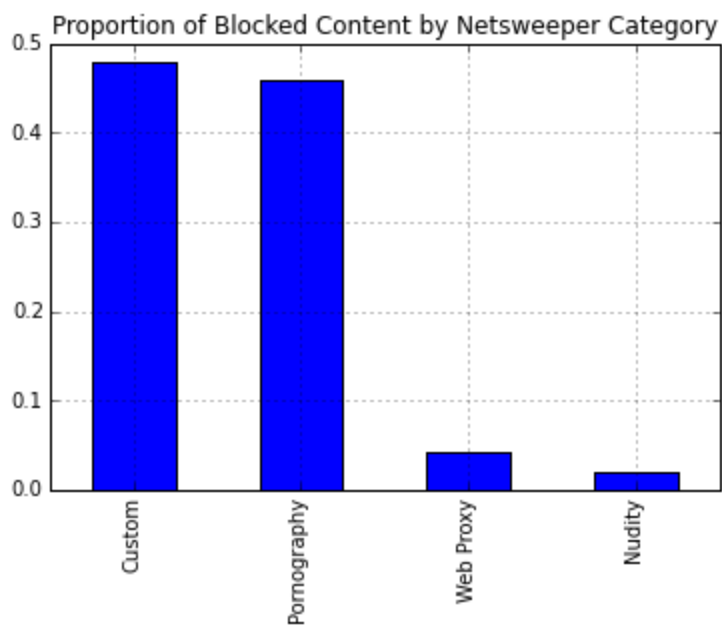


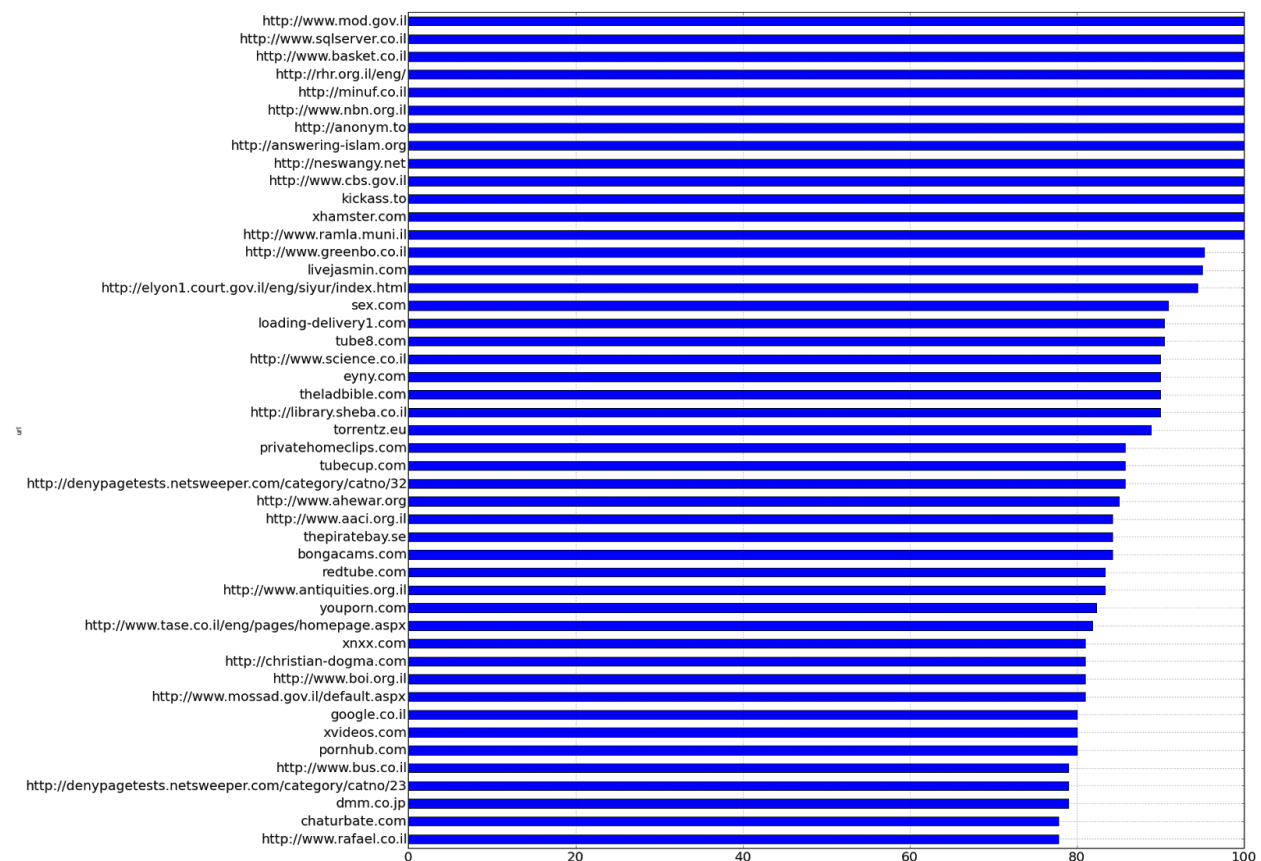
Figure 18: Proportion of all URLs found blocked belonging to the four blocked content categories

The Custom category contained primarily URLs belonging to the Israel ccTLD (more about this below) as well as three additional URLs:

1. <http://www.ahewar.org>
2. <http://answering-islam.org>
3. <http://christian-dogma.com>

We discuss the blocked content in more detail later in this report.

There was some variability in filtering across the testing time period. For those URLs found blocked with a Netsweeper blockpage, the proportion of tests for which that URL was found to be blocked ranged from 78% to 100%, as shown in Figure 19:



*Figure 19: Proportion of tests in which each URL was found to be blocked, out of all URLs that triggered a Netsweeper blockpage at least once.*

It is not clear why certain URLs were accessible during a small number of tests. [Previous research by ONI](#) identified a lack of concurrent Websense user licenses as the reason why blocking was intermittent: when the number of users accessing the Internet exceeded the limited number of user licenses, no blocking was applied. It is unknown whether a similar limitation with the Netsweeper installation is the cause of this variability. We also searched for but did not find a conclusive link between reports of network disruptions and variability in filtering.

### Non-transparent blockpage

In addition to the transparent Netsweeper blockpage, during our attempts to access other types of content we were presented with the page displayed in Figure 20:

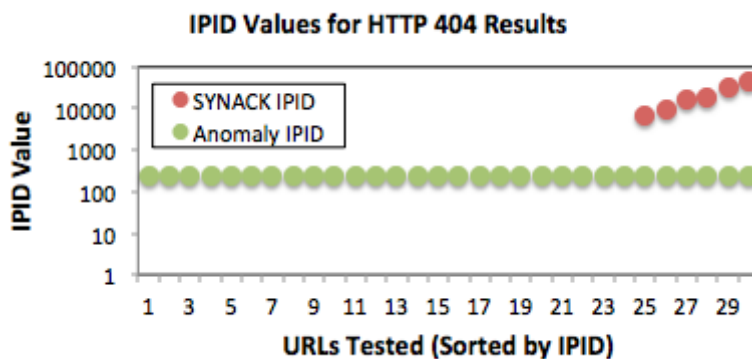


*Figure 20: HTTP 404 error displayed during an attempt to access sahafah.net on YemenNet*

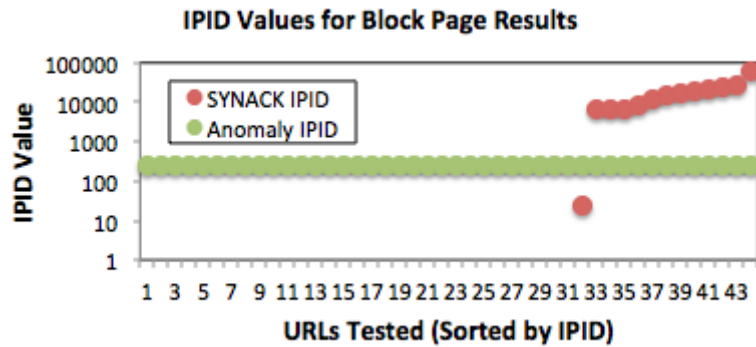
This HTTP 404 error page is a standard server error and is not, on its own, indicative of censorship. However, a number of characteristics of the response seen in Figure 20 reveal it is in fact a result of deliberate censorship.

Interestingly, we found evidence that the HTTP 404 messages originated from the same device as the Netsweeper blockpage. This finding is significant, as it suggests that the Netsweeper installation is responsible for both the transparent and nontransparent blockpages. To ascertain that these replies indeed originated from the same device in the network, we considered the values of the IPID and TTL headers in the HTTP responses. We leverage the value of these headers as seen in the TCP SYNACK packet as a baseline to compare against. The SYNACK packet represents the first response received by the client from the server, and (if a packet injecting censor is slow to act) the SYNACK packet can give us insight into how the actual server sets these header values.

IPID header comparison. The IPID header can be set differently depending on the operating system of the device that generates the network packet (e.g., some will set it to 0, while others may increment it based on packets sent). We compared the IPID values between the SYNACK packet, presumably the first reply from the server, and the packet containing the HTTP response. Figure 21 shows the result. In the SYNACK packet, the majority of servers set the IPID value to 0 (not shown on the logscale figure). In contrast, the IPID in the packet containing the HTTP reply (either HTTP 404 or blockpage) was consistently set to the value of 242. This very consistent and specific setting of the IPID header is in line with the same device being used to generate both the HTTP 404 and blockpage responses. In the case of HTTP 404 responses, the difference in IPID between the SYNACK packet and the HTTP reply also corroborates that it is not the actual web server generating the HTTP 404 response.



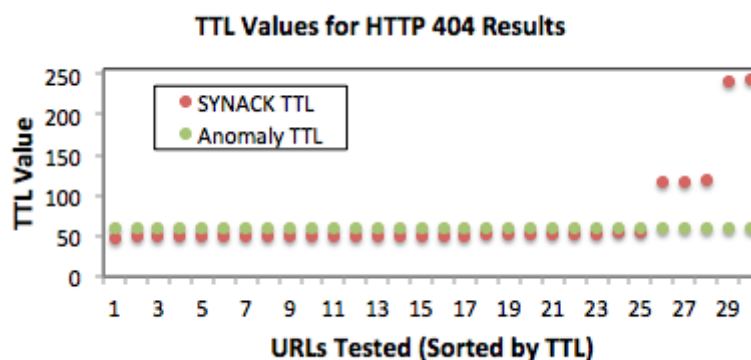
a. IPID Values for tested URLs that resulted in an HTTP 404 page being returned



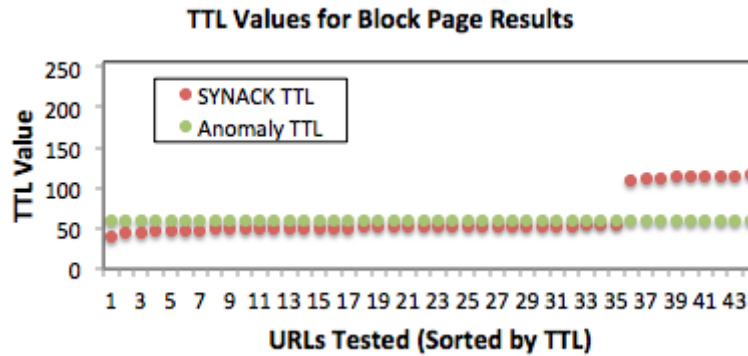
b. IPID values for tested URLs that resulted in a blockpage being returned

Figure 21. Comparison of IPID values between the initial response from the server (the TCP SYNACK packet) and the response carrying the HTTP 404 or blockpage result. Note the consistent IPID value of 242 between the HTTP 404 and blockpage results.

TTL header comparison. The IP TTL header is initially set to a value of 255 (or 128) and decremented at each hop as a packet traverses the network. The TTL value can give us a hint at how far the server is from the client (in terms of routers). Figure 22 compares the TTL values between the SYNACK packet and the packet containing the HTTP reply. We see the TTL values for SYNACK packets ranged from 40 and 55 (for sites that were hosted outside of the Middle East), around 100 for sites hosted in the Middle East (e.g., Israel) and 200 for sites hosted in Arab countries. In contrast, we observed a consistent TTL value of 60 for the packets containing the HTTP 404 or blockpage replies. This finding provides further evidence that these responses are generated by a device located at the same point in the network. Again, the difference between the SYNACK packet and HTTP 404 response indicates that these responses were not generated by the web server in the case of the 404 response.



a. TTL values for URLs that resulted in an HTTP 404 page being returned



b. TTL values for URLs that resulted in a blockpage being returned

Figure 22: Comparison of TTL values between the initial response from the server (the TCP SYNACK packet) and the response carrying the HTTP 404 or blockpage result. Note the consistent TTL value of 60 between the HTTP 404 and blockpage results.

This specific HTTP 404 error response was received exclusively during attempts to access Yemen-focused critical news websites. Further analysis of the blocked content can be found below.

Our test results showed that this response was not consistent across all tests. Some URLs received this response during every test, while for others there were periodic instances in which the website was accessible. In some cases the website was accessible for only one or two tests, while in others the URL was accessible during most tests until it appears to have been added to the list of blocked content during later tests. The following table displays the URLs that received the HTTP 404 error, and the percentage of tests in which this response was received:

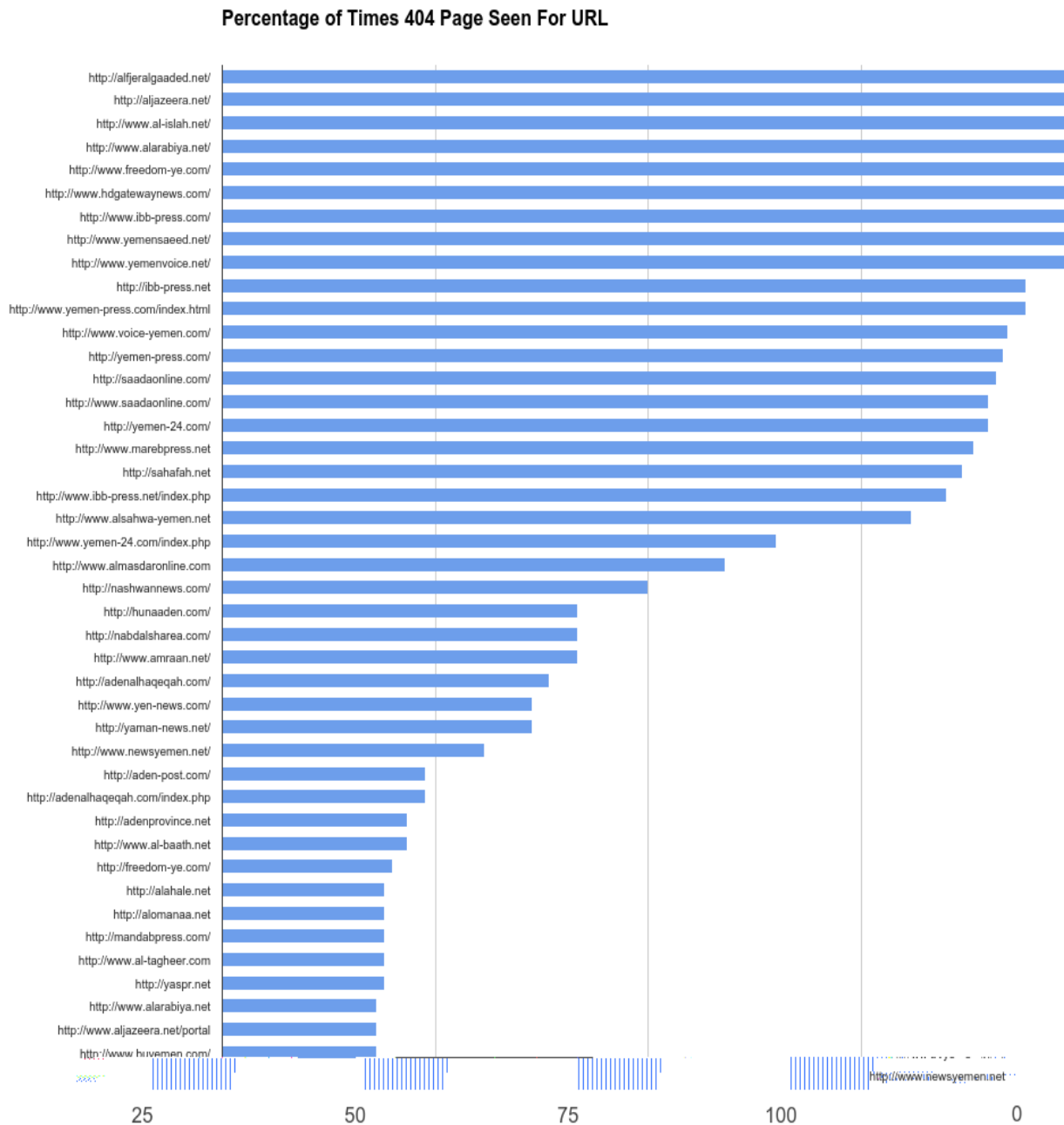


Figure 23: Proportion of tests in which URLs blocked at least once with HTTP 404 error were blocked

As with the results seen with the transparent Netsweeper blockpage, as shown in Figure 19, it is not clear why certain URLs were accessible in some tests and blocked during others.

Additional network scans

In addition to tests of website accessibility in Yemen, we also conducted remote network scans of the YemenNet network to identify filtering infrastructure, and to provide further confirmation of Netsweeper's products.

First, we used Shodan, a search engine that provides information on devices connected to the Internet. We have previously used Shodan to identify the presence of [Netsweeper devices in Somalia](#) and [Pakistan](#). Using the IP we see explicitly in the blockpage (82.114.160.94) as a starting point, Shodan shows the following string in its SNMP description:

```
Linux localhost.localdomain 2.6.32-358.2.1.el6.x86_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013  
x86_64
```

This Linux kernel version number is consistent with the naming scheme of the Linux distribution [CentOS](#), which Netsweeper is built upon. After searching for the string “2.6.32-358.2.1.el6.x86\_64” and restricting the results to Yemen, Shodan identified the devices shown in Figure 24:

Showing results 1 - 10 of 10

**82.114.160.101**

**TeleYemen**

Added on 2015-06-14 00:22:20 GMT

 Yemen

[Details](#)

Linux NS-PS06 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.94**

**TeleYemen**

Added on 2015-06-13 19:03:54 GMT

 Yemen

[Details](#)

Linux localhost.localdomain 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.102**

**TeleYemen**

Added on 2015-06-08 12:23:04 GMT

 Yemen

[Details](#)

Linux webadmin01 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.97**

**TeleYemen**

Added on 2015-06-06 21:40:25 GMT

 Yemen

[Details](#)

Linux NS-PS02 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.98**

**TeleYemen**

Added on 2015-06-05 00:29:28 GMT

 Yemen

[Details](#)

Linux NS-PS03 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.99**

**TeleYemen**

Added on 2015-06-03 05:38:01 GMT

 Yemen

[Details](#)

Linux NS-PS04 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.103**

**TeleYemen**

Added on 2015-06-02 19:01:15 GMT

 Yemen

[Details](#)

Linux webadmin01 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

**82.114.160.104**

**TeleYemen**

Added on 2015-06-02 06:26:54 GMT

 Yemen

[Details](#)

Linux webadmin02 2.6.32-358.2.1.el6.x86\_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86\_64

*Figure 24: Shodan search results for devices returning CentOS version string in Yemen*

We then verify each IP by opening them in a browser and ensuring that the signature of the URL pattern “/webadmin/” is present, as well as visiting the IPs to verify the default Netsweeper content is present. Based on these results we are able to sketch out an illustration of the Netsweeper infrastructure, as shown in Figure 25:

## Netsweeper Infrastructure in YemenNet

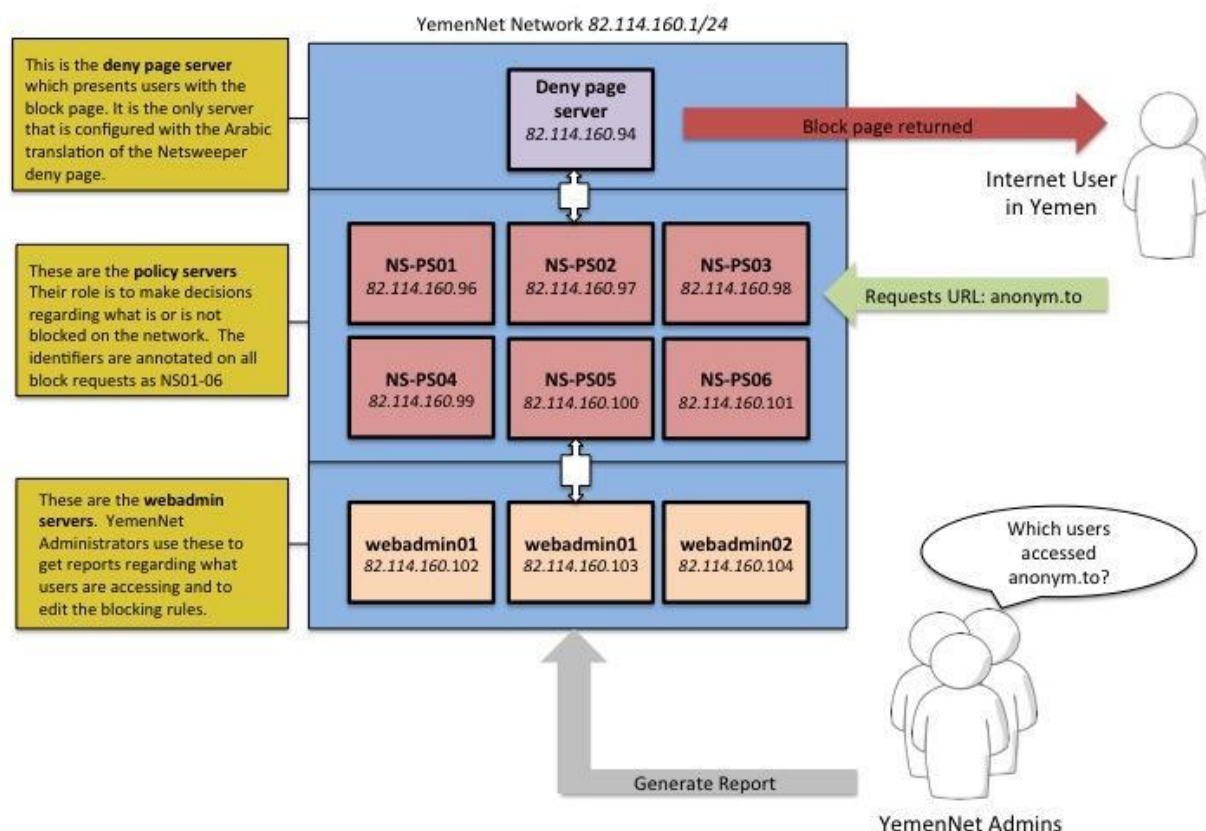


Figure 25: Illustration of YemenNet's Netsweeper filtering infrastructure

There are three main components to the Netsweeper installation in YemenNet: a single deny page server that presents the blockpage to users; six policy servers that make the decision about what to block; and three servers dedicated to the web interface that administrators use to set new filtering policies and get reports about user traffic.

The deny page server is hosted on 82.114.160.94 and is seen in the source code of any blockpage as an embedded iframe, as described earlier in this report. There are two configurations that suggest that the primary use of this server is to serve blockpages. First, Netsweeper blockpages are served according to a deny page ID parameter (dpid) in the URL. For example, a block URL formatted as `'http://127.0.0.1/webadmin/deny/index.php?dpid=1'` would serve one blockpage while

[‘http://127.0.0.1/webadmin/deny/index.php?dpid=2’](http://127.0.0.1/webadmin/deny/index.php?dpid=2) would serve another. The blockpage we identified on YemenNet uses the value ‘dpid=5’ which presents the customized block message in Arabic shown in Figure 16. Of all the Netsweeper devices identified, only 82.114.160.94 has a custom blockpage with Arabic text. The other Netsweeper servers found on this network have only the default Netsweeper blockpages. Another factor that suggests that this server’s only function is to serve the blockpage is that this is the only server we identify that has HTTPS disabled and serves the blockpage entirely unencrypted over port 80. Port 443 is open on this IP but serves no content, and it is the only Netsweeper server identified here configured as such. In our testing data, we only saw this one IP serve the blockpage and it was always served unencrypted over port 80. YemenNet administrators may have disabled SSL encryption for the blockpage in an effort to reduce the bandwidth needed to serve blockpages to its customers.

A policy server, as described by Netsweeper’s [documentation](#), “categorizes the (user’s) request, maps the requests to a policy, and determines whether the request should be allowed or blocked.” We are able to identify the use of six different policy servers, as the blockpage URL annotates which server made the decision in each of the blockpages it serves. For example, a sample blockpage found in our tests on YemenNet looked as follows (emphasis added):

<http://82.114.160.94/webadmin/deny/?dpid=5&dpruleid=3&cat=23&ttl=-200&groupname=default&policyname=default&username=-&userip=X.X.X.X&connectionip=127.0.0.1&nsphostname=NS-PS03&protocol=policyprocessor&dplanguage=-&url=http%3a%2f%2fplayboy%2ecom%2f>

Our test results identify six different policy servers, ranging from NS-PS01 to NS-PS06. We see these hostnames in our SHODAN results on YemenNet, all of which run Netsweeper, sequentially in the IP range from [82.114.160.96](#) (NS-PS01) to [82.114.160.101](#) (NS-PS06). Given that they are annotated in each blockpage (as *nsphostname*) and that the name is NS-PS01 we can infer these are the Netsweeper policy servers and that there are six active servers in this infrastructure.

Our test results show which policy servers were used most often for processing blocking decisions, as shown in Figure 26:

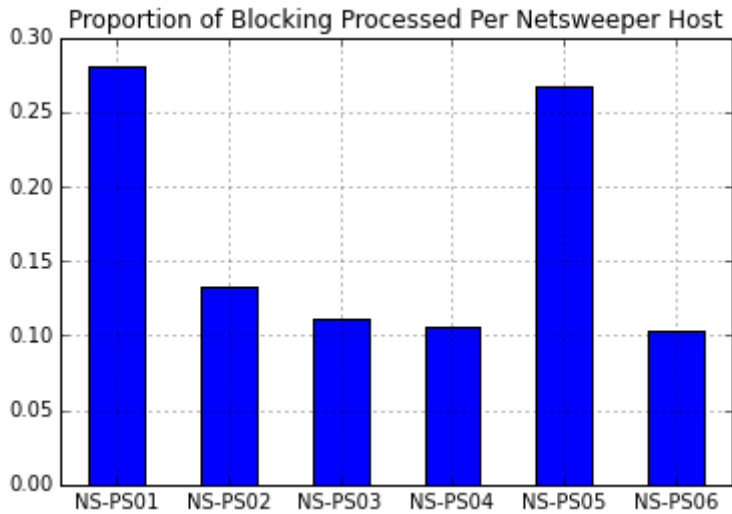


Figure 26: Proportion of blocking performed per YemenNet Netsweeper host

The final component we see are three sequential IPs ([82.114.160.102](#) to [82.114.160.104](#)); two with the hostnames of 'webadmin01', and one with a hostname of 'webadmin02'. The names suggest that these are functioning as the webadmin component of Netsweeper. According to [Netsweeper documentation](#), webadmin is a “web-based administration module that is used to manage all aspects of the Netsweeper platform including: creating policies, managing users, generating reports, updating system access rights, monitoring system usage, etc.” This is the part of the system that administrators would interact with in order to change what is filtered as well as to generate reports about which users are accessing blocked content.

In totality, these three components and 10 servers encompass the blocking infrastructure present in YemenNet.

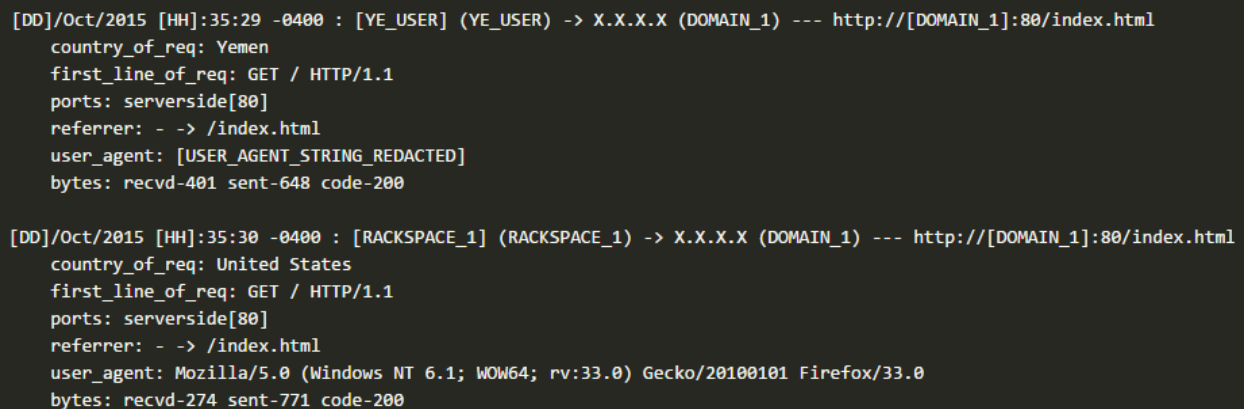
Are Netsweeper devices in Yemen communicating with Netsweeper-controlled servers in North America?

As has already been described, Netsweeper’s filtering process assigns all URLs to a category based on content, and allows system administrators to either permit or deny users from accessing URLs in that category. Given the enormous volume of potential URLs which may be accessed and thus need to be categorized, part of Netsweeper’s service offerings include linking a customer’s installation to the company’s master database of categorized URLs.

The process works as follows: If a user in Yemen accesses a URL which is not in the database (and thus has not been categorized) by the Yemeni Netsweeper installation, the system in Yemen will communicate with Netsweeper's Master Category Name Server, which "[is hosted on the Internet by Netsweeper.](#)" This Netsweeper hosted server accesses the URL, performs an automated analysis of the site's content in order to categorize it, and returns that categorization to the local Netsweeper installation. The [company's documentation](#) says that the "entire Netsweeper categorization process—from initial outgoing Internet request for a URL never seen by the system before (worldwide) to Categorization Engine categorization and storage in the database—takes as little as one second and at most about five seconds."

We sought to determine if YemenNet's Netsweeper installation was actively communicating with and receiving service from Netsweeper. We attempted to confirm this by creating new, uncategorized websites, accessing them from YemenNet and examining requests for those websites. We registered 6 domains which hosted innocuous content on servers we controlled. A user of YemenNet located in Yemen then accessed 3 of these domains, while the remaining 3 acted as a control and were only accessed outside of Yemen. We then observed the server logs to identify what content was requested and where the requests came from.

In all 3 non-control cases, the server logs show the YemenNet user accessing the test domain, followed less than a second later by another request for the same content, as shown below in Figure 27:



```
[DD]/Oct/2015 [HH]:35:29 -0400 : [YE_USER] (YE_USER) -> X.X.X.X (DOMAIN_1) --- http://[DOMAIN_1]:80/index.html
country_of_req: Yemen
first_line_of_req: GET / HTTP/1.1
ports: serverside[80]
referrer: - -> /index.html
user_agent: [USER_AGENT_STRING_REDACTED]
bytes: recvd-401 sent-648 code-200

[DD]/Oct/2015 [HH]:35:30 -0400 : [RACKSPACE_1] (RACKSPACE_1) -> X.X.X.X (DOMAIN_1) --- http://[DOMAIN_1]:80/index.html
country_of_req: United States
first_line_of_req: GET / HTTP/1.1
ports: serverside[80]
referrer: - -> /index.html
user_agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
bytes: recvd-274 sent-771 code-200
```

*Figure 27: Server log files showing request for test domain from Yemen followed less than 1 second later by a request from a Rackspace-hosted IP address. (Note: Identifying information has been redacted from this image)*

All three requests, corresponding to the 3 test domains, came from IP addresses hosted by [Rackspace](#), a large US-based cloud service and hosting company. None of the 3 control domains were visited by Rackspace IP

addresses. While the Rackspace IP addresses differed, the requests, including user-agent string and all requesting headers, were identical. Additional attempts to access the 3 test domains from Yemen the following day were not followed by requests from Rackspace-hosted IP addresses.. This was expected behaviour, as the Netsweeper installation in Yemen would already have the category for this URL and would not need to fetch it again. In addition, attempts to access these websites from an ISP which does not use Netsweeper were not followed by requests from Rackspace-hosted IP addresses.

This precise set of actions -- an uncategorized website is accessed by a Rackspace IP address request within a second it being accessed on an ISP using Netsweeper -- was [described by a user](#) of the Australian ISP Telstra, which were later acknowledged by Telstra as [the process by which their Netsweeper installation categorizes previously unseen URLs](#).

While we cannot definitively link these requests from Rackspace-hosted IP addresses to YemenNet's Netsweeper installation, the behaviour we identified was consistent with previous reports of Netsweeper installations categorizing unseen URLs. These tests show it is highly likely that Netsweeper infrastructure is communicating with and providing services to the YemenNet Netsweeper installation.

## Overview of content blocked in Yemen

We turn now from analysis of the blocking system to the type of content targeted for blocking in Yemen. Content found blocked on YemenNet included local news websites providing news and views on the armed conflict in the country. These sites cover news about the ongoing armed conflict between the Houthi rebels and their allies on one side, and supporters of President Hadi (known as the Popular Resistance Committees) aided by Saudi-led airstrikes on the other. The websites highlight the atrocities of the war and civilian casualties caused by both sides. Blocked sites address, *inter alia*, how the war has exacerbated the humanitarian crisis through deterioration of health services, due to the electricity cuts and shortage of fuel needed to operate hospitals and health centers; citizens' inability to travel due to the lack of fuel for vehicles; and the impact of the war on the local economy and employment.

Though such coverage is available on websites that remain accessible, the blocked websites appear to have been blocked because they publish reports and op-eds that are particularly explicit in criticising the Houthi rebels, accusing them of triggering the war by taking over the capital and expanding to other provinces by force. Generally speaking, the reports and op-eds on the blocked websites seem to be supportive of the government of President Hadi, which is recognized regionally and internationally as the legitimate

government of Yemen, and they do not recognize the constitutional declaration announced by the Houthis to formally take control of the government. For example, one of the blocked websites features on its [home page](#) photos of lead politicians who have been arrested by the Houthis and another one has [published](#) (in Arabic) a report about civil society organizations documenting alleged human rights violations and atrocities committed by the Houthis. Another blocked website published an [opinion piece](#) (in Arabic) in which the writer calls for dissolving the political party GPC, which is headed by the Houthis' ally former president Saleh, for collaborating with the Houthi militias. Another website has [reported on the number of Houthi casualties](#) in the armed conflict. Finally, a blocked [news portal](#) aggregates stories from many of the other blocked local media websites.

The vast majority of the blocked websites are local news portals and websites of local newspapers and media outlets as well as websites of local political parties. Websites of two pan-Arab news websites appear among the blocked list: the website of Aljazeera TV station and the website of Al-Arabiya TV station.

With the exception of URLs belonging to the Israel TLD (described below), most filtering of news and political content is non-transparent. The '404 Not Found' page returned appears to be an attempt to mislead users into thinking particular websites are inaccessible for technical reasons rather than intentionally blocked.

URLs from three other categories not specific to Yemen (Pornography, Nudity, and Web Proxy) were also found blocked, all via the Netsweeper blockpage. Among those URLs were two diagnostic websites used for troubleshooting a Netsweeper installation:

<http://denypagetestsnetsweeper.com/category/catno/32>

<http://denypagetestsnetsweeper.com/category/catno/23>

These two URLs are both created by Netsweeper and have been categorized by the company as the content categories Web Proxy (32) and Pornography (23), respectively. They are meant to be used by systems administrators to determine if the correct content categories are being blocked on their installations. The fact that these URLs are blocked is further confirmation that Netsweeper is being used by YemenNet. The 'deny page test' URL for the category 'Nudity' (3) is also likely blocked, however, it was not on the testing list at the time of testing.

Filtering of all Israel top level domain URLs

One of the key findings of these tests is that all Israel top-level domain (.il) URLs tested (with one special exception) were found to be blocked (listed below). The testing list contained 25 URLs belonging to this TLD, which represented a range of different content types, from the website of the Mossad to the Israel Basketball League. All but one of these URLs are found to be blocked using the Netsweeper blockpage. The sole exception is the URL '<http://thissitedoesnotexist.il>', which is not a registered domain. We hypothesize that as the DNS lookup did not complete successfully, the request did not reach the Netsweeper device.

Previous [ONI test results from Yemen](#) have not shown any evidence that .il websites were blocked. The Houthis, who control YemenNet, [use the slogan “Death to America, Death to Israel, A curse upon the Jews! Victory for Islam!”](#) and they have displayed the slogan in areas under their control. They have also printed the slogan on walls of institutions they run such as YemenNet as shown in Figure 28 below. Interestingly, [Iran is another country that blocks all URLs using the Israel ccTLD](#). This raises the question whether the Houthis, who control the ISPs in Yemen undertaking the blocking and [share the Shiite ideology with and receive military support from Iran](#), are aligning their censorship policy with the censors in Iran.



*Figure 28: YemenNet’s front gate. The Houthis’ slogan is visible to the left and right of the gate, printed on the wall in green and red. The slogan says “Allah Akbar; Death to America, Death to Israel, A curse upon the Jews! Victory for Islam!” (Photo credit: Naser Noor)*

The blocking of all .il URLs is an intriguing development that implies objection to the state of Israel, with which Yemen does not have diplomatic relations. The previous government of Yemen, during the regime of ex-president Saleh, did not block .il websites despite the fact that there has never been diplomatic relations between the two states. Other Arab states that do not have formal diplomatic relations with Israel (e.g., [Saudi Arabia](#)) do not block all .il websites. Interestingly, YemenNet renders its standard explicit blockpage for .il websites, which suggests that the censors are open about this particular policy. See Figure 29 for an example.

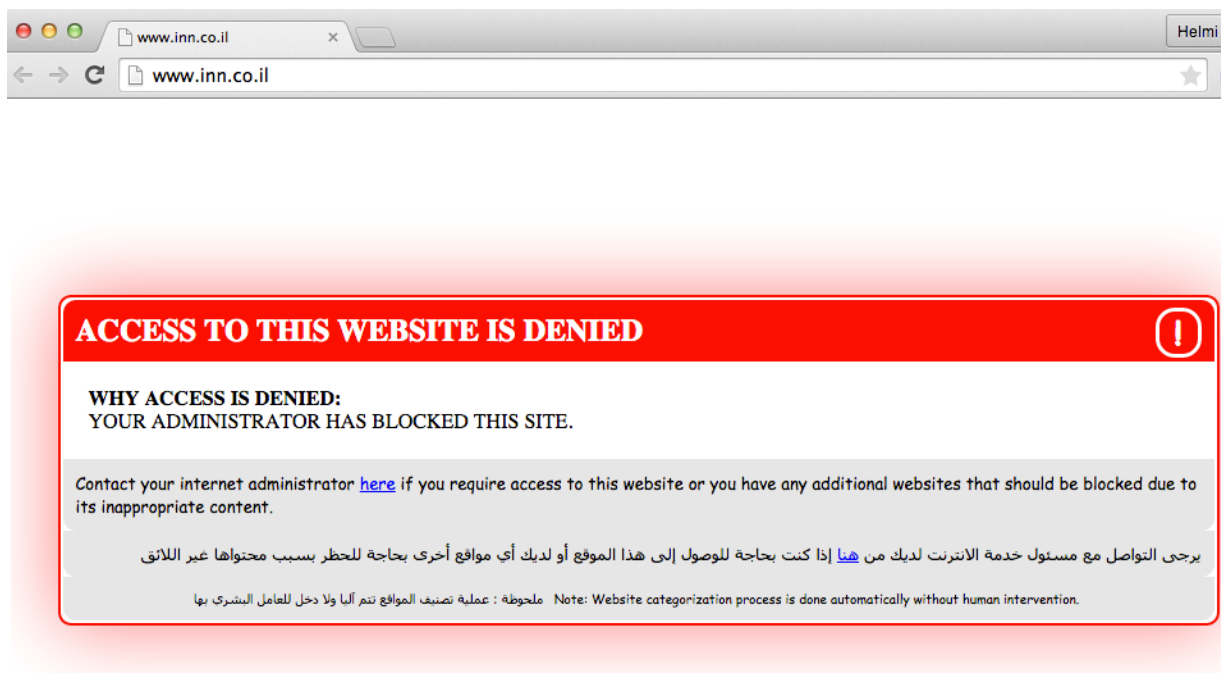


Figure 29: Screen shot showing blocking of an Israel top level country domain name with Netsweeper blockpage.

The following URLs belonging to the Israel TLD were blocked using a Netsweeper blockpage:

1. <http://elyon1.court.gov.il/eng/siyur/index.html>
2. <http://library.sheba.co.il>
3. <http://minuf.co.il>
4. <http://neswangy.net>
5. <http://rhr.org.il/eng/>

6. <http://www.aaci.org.il>
7. <http://www.ahewar.org>
8. <http://www.antiquities.org.il>
9. <http://www.basket.co.il>
10. <http://www.boi.org.il>
11. <http://www.bus.co.il>
12. <http://www.cbs.gov.il>
13. <http://www.greenbo.co.il>
14. <http://www.mod.gov.il>
15. <http://www.mossad.gov.il/default.aspx>
16. <http://www.nbn.org.il>
17. <http://www.rafael.co.il>
18. <http://www.ramla.muni.il>
19. <http://www.science.co.il>
20. <http://www.sqlserver.co.il>
21. <http://www.tase.co.il/eng/pages/homepage.aspx>

#### Other content categories blocked in Yemen

Test results reveal that YemenNet continues to block websites from various categories as has been previously documented by [ONI](#). Examples include content that is critical of Islam (e.g., <http://answering-islam.org>), sex and pornography websites (e.g., [playboy.com](http://playboy.com)) and privacy and anonymization tools websites (e.g., <http://anonym.to>).

#### Corporate social responsibility implications of Netsweeper services to YemenNet

As Citizen Lab has explored in a number of reports, Internet filtering technology is inherently “dual use” -- that is, it may serve legitimate and socially beneficial purposes such as traffic management, but may also be put to more nefarious ends, including the curtailing of information and services that would enable citizens to hold regimes accountable and effectively communicate. Private sector entities that supply such technology are in a difficult position, as they must consider the potential human rights impact of their services without themselves acting as unaccountable arbiters of what content is appropriate or properly circumscribed under relevant law. A number of companies have publicly struggled with these issues, for example, Websense, which developed an [anti-censorship policy](#).

Despite the complexity of these problems, companies have the responsibility at all times to respect human rights. The [UN Guiding Principles on Business and Human Rights](#) note as a basic foundational principle, “Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.” Furthermore, companies should “[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts” – which requires proactive efforts with respect to clients utilizing their services.

In the case of Netsweeper’s provision of services to YemenNet, it is clear that under the control of the Houthis the ISP has used Netsweeper technology in a manner that adversely impacts human rights. Through its Netsweeper installation, YemenNet has censored news and opinion related to the conflict, undermining users’ rights under Article 19 of the [International Covenant on Civil and Political Rights](#) (ICCPR) to hold opinions without interference and “to seek, receive and impart information and ideas of all kinds.” Moreover, Netsweeper technology is employed to filter *any* content originating from an Israeli top-level domain (.il), in blatant violation of international human rights law. The UN Human Rights Committee has noted in its [General Comment No. 34](#), regarding application of ICCPR Article 19, that:

*Any restrictions on the operation of websites, blogs or any other internet-based electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 [of ICCPR Article 19, which provides that restrictions on the right to freedom of opinion and expression may be permissible if they are provided by law and are necessary for respect of the rights or reputations of others, or for the protection of national security or of public order, or of public health or morals]. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.*

According to the Committee’s reasoning, a generic ban of an entire swath of content on the basis of its ccTLD, regardless of its actual content, is *never* permissible under the ICCPR. It is therefore incumbent upon Netsweeper to prevent such use of its technology in order to fulfill its corporate responsibility to respect human rights.

Citizen Lab sent a letter to Netsweeper on October 9, 2015 inquiring about the use of its products by YemenNet; [the letter is reproduced here](#). Our letter raises questions regarding Netsweeper's due diligence to maintain knowledge of the end user and end uses of its technology in Yemen, an active conflict zone; its lack of policy statement and continued silence on the human rights impacts of its products and services; and its ability to design or control its technology in a manner that prevents certain human rights abuses. As of October 20, 2015, we have not received a reply to this letter.

## b. Saudi Arabia

In April 2015, [Yemeni media reports](#) suggested that Saudi Arabia had blocked Yemeni government and news websites controlled by the Houthis or affiliated with ousted president Saleh. We conducted tests of a list of relevant websites (a full testing list can be found in the data section below) to confirm this new blocking.

We performed testing using the ICLab platform on VPNs based in Saudi Arabia. Testing was conducted on a commercial VPS provider which gets Internet connectivity from Saudi Telecom Company. Testing was conducted using two testing lists: first, a list of 401 URLs containing sites related to Saudi Arabia's domestic political, religious and cultural context, as well as a sampling of Yemen-related news websites and sites belonging to the Israel .IL ccTLD; second, the Alexa Top 500 URLs worldwide. In total, 901 URLs were tested in Saudi Arabia.

Our test results confirmed user reports of Yemen-related content, amongst other types of content, being blocked in Saudi Arabia. Our testing identified two distinct blockpages, as shown in Figure 30 and Figure 31:

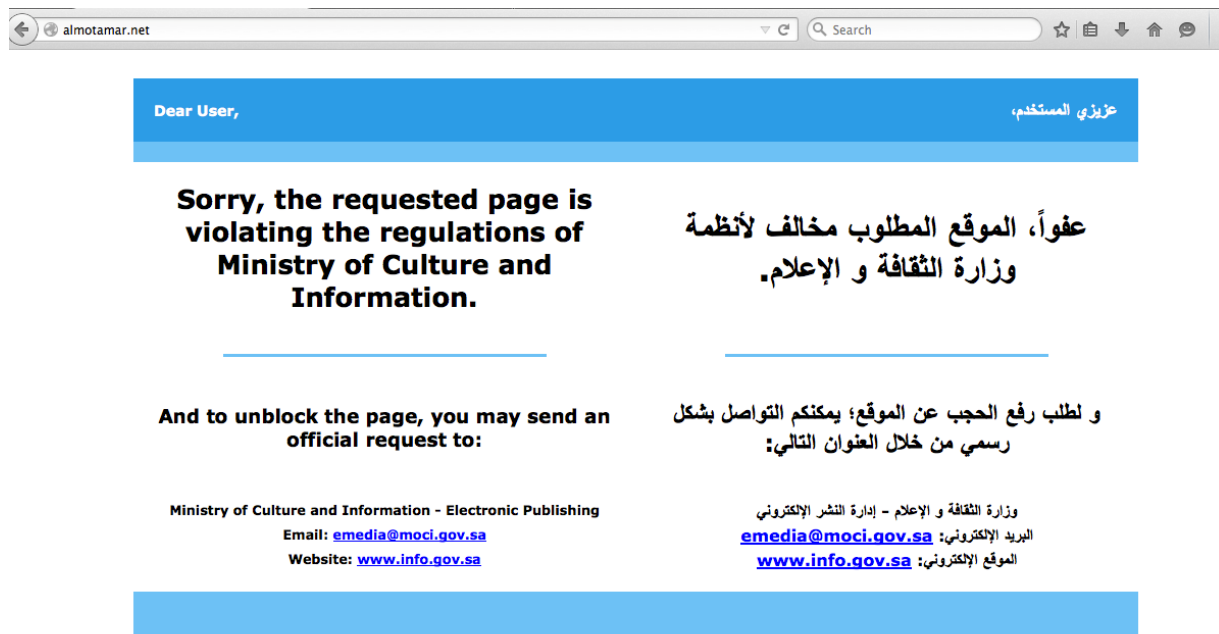


Figure 30: “Blue” blockpage displayed in Saudi Arabia when accessing blocked content

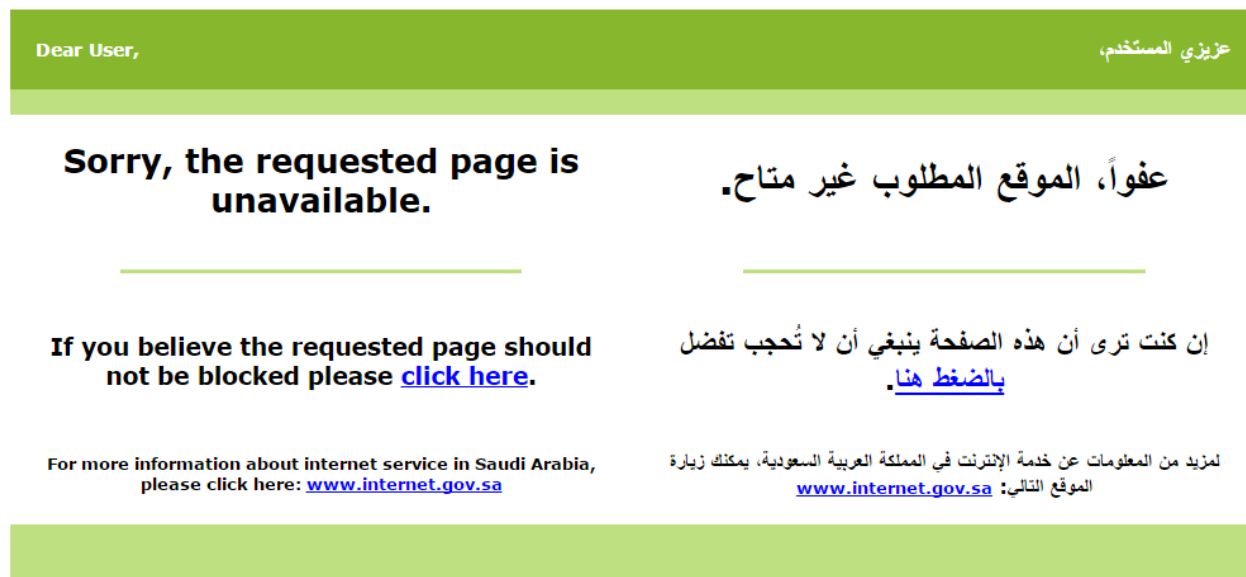


Figure 31: “Green” blockpage displayed in Saudi Arabia when accessing blocked content

Both blockpages indicate that they are being generated by [Wirefilter](#), a filtering product developed by Saudi-based company Sewar Technologies. The headers returned with the blockpage contain additional information which, in a similar manner to the Netsweeper hostnames described above, further identify the different devices which make up the Wirefilter infrastructure. For example, the one header returned with the

blockpage says: “Protected by WireFilter 8000 (RY-WF01-FB03)” in the server tag. It is likely that the 10 digit code (“RY-WF01-FB03”) identifies the specific device used to perform filtering or return the blockpage. In total, we identified 7 unique header responses:

1. WireFilter
2. WireFilter 8000 (RY-WF02-FB01)
3. WireFilter 8000 (RY-WF01-FB02)
4. WireFilter 8000 (RY-WF01-FB03)
5. WireFilter 8000 (RY-WF02-FB03)
6. WireFilter 8000 (RY-WF01-FB01)
7. WireFilter 8000 (RY-WF02-FB02)

There was variation in the types of content which led to the green blockpage and those which triggered the blue blockpage. In total, 10 unique URLs triggered the blue blockpage and 103 URLs triggered the green blockpage. The full list of blocked URLs can be found below in the Data section.

### **Overview of blocked content in Saudi Arabia**

The blocked websites which triggered the blue blockpage were websites which disseminate the Houthi narrative on the military and political conflict in Yemen and provide hostile views towards the Saudi government, particularly since the Saudi-led airstrikes began. These websites included the Yemeni government news agency Saba News (<http://sabanews.net>) which is controlled by the Houthis; the websites of Al-Thawra, a Yemeni government newspaper (<http://www.althawranews.net>) also controlled by the Houthis; the website of the former ruling party General People’s Congress (GPC), which is led by Saleh (<http://almotamar.net/news/>); the website of TV channel Yemen Today (<http://www.yementodaytv.net>), which is owned by Saleh; and the news portal Khabar Agency (<http://khabaragency.net>) which is affiliated with the GPC. The list of URLs blocked with the blue blockpage was not exclusively political in nature -- file-sharing site The Pirate Bay was also blocked with this blockpage.

More websites were blocked after our first test runs. They include the website of the government newspaper 26 September (<http://www.26sep.net>), which is under the control of the Houthis, the website of Houthi TV station Al-Masirah (<http://www.almasirah.tv/>), which live streams its broadcast, and Ansar Allah (<http://ansar-allah.net>), which disseminates news and views of the Houthi rebels. Also blocked is the news website Saadah Press (<http://www.saadahpress.net>) and Masa Press (<http://masapress.net/>), both of which have content aligned with the Houthis and GPC.

Interestingly, we found a number of Iranian news websites to be blocked. These include the websites of Al-Alam News Network (<http://www.alalam.ir>), which is Iran's state news TV station; Iran Republic News Agency (<http://www.irna.ir/en>) and Fars News (<http://arabic.farsnews.com>). Iranian media report news sympathetic to the Houthis. As mentioned above, Saudi Arabia has accused Iran of supporting the Houthis militarily.

Other websites found blocked in Saudi Arabia include content categories which we previously found to be blocked as part of our research on [ONI](#). They include pornography, LGBT content, circumvention tools, file-sharing sites, as well as critical religious and political content.

The blocked websites which triggered the green blockpage included a broader variety of content categories, including pornography, LGBT content, circumvention tools, file-sharing sites, as well as critical religious and political content not related to Yemen.

### c. Iran

As a result of the reports linking Iran to the conflict in Yemen, we conducted additional network measurement testing in Iran to identify instances of filtering relevant to the conflict. We tested on a publicly available VPN, using a testing list containing Saudi news websites, a sampling of .IL URLs, as well as the Alexa Top 500 websites.

We performed testing using the [ICLab platform](#) on a VPN based on the ISP Soroush Rasaneh, as well as some follow-up testing on a commercial VPS provider in Iran. The full list of URLs tested can be found in the Data section below. In total, 655 URLs were tested on this ISP in Iran.

Our test results confirmed instances of blocking on this ISP in Iran. Test results identified 211 URLs which returned the blockpage shown in Figure 32:



Figure 32: Blockpage identified in Iran

This blockpage had the following source:

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=windows-1256"><title>M1-6</title></head><body><iframe src="http://10.10.34.34?type=Invalid Site&policy=MainPolicy \" style="width: 100%; height: 100%" scrolling="no" marginwidth="0" marginheight="0" frameborder="0" vspace="0" hspace="0"></iframe></body></html>
```

### Overview of content blocked in Iran

Our test results confirmed instances of Saudi Arabia-related blocking in Iran, as well as blocking of content related to Israel. Among the blocked content is the website of Saudi-owned pan-Arab TV station Al-Arabiya (<http://alarabiya.net>), which we found to have been blocked in Yemen after the Houthis have taken over government institutions. Also blocked are Saudi newspapers Al-Riyadh (<http://www.alriyadh.com/>) and Al-Yaum (<http://www.alyaum.com>), Saudi-owned pan-Arab newspaper Asharq Al-Awsat (<http://aawsat.com>), and Saudi newsportal Sabq (<http://sabq.org>).

We also found that a major Yemeni news website, Mareb Press (<http://marebpress.net/>) is blocked in Iran. Interestingly, this website is among those blocked in Yemen by YemenNet, which is under the control of Houthis. Also, we found all Israel top level domain names (.il) blocked in Iran including websites that do not have political or social content, such as a bus service information website (<http://www.bus.co.il>). Thus Iranian content filtering practices towards Israeli domains are identical to those implemented by YemenNet under control of the Houthis.

We also found that Iran continues to block various content in different categories as has been previously documented by [ONI](#).

## Discussion and Conclusion

---

Control of information has always been an important ingredient of armed conflict, but has taken on special importance in the digital age. Parties to an armed conflict now fight over information as much as they do other material resources, and attempt to control the means of communication in their favour just as they attempt to gain air superiority or control over critical sea lanes. However, research on information controls during an armed conflict presents special challenges. Just as the "fog of war" makes it difficult for commanders to make informed decisions based on situational awareness, so does it make it difficult for researchers to trace the dynamics of the information environment through careful evidence-based analysis. In the midst of a war it is difficult to distinguish deliberate attempts to control information through disruption or control of the supply of resources needed to power media or telecommunications from accidents of warfare or collateral damage. Adding to the challenges are the security risks that research in zones of conflict presents. Throughout this case study we faced ongoing concerns about the safety of the in-country researcher with whom we collaborated, debated the ethics of undertaking network measurement in an environment of high risk, and ceased testing altogether as a result of these concerns.

In this case study, we find that the Houthis undertook a concerted effort to shape the information environment in Yemen to their advantage by shutting down local media, increasing Internet filtering, and limiting the supply of oil necessary to power infrastructure -- what might be best described as a strategy of "information denial" in line with the Houthis' extreme ideology. Coincidentally, collateral disruptions to electricity and other infrastructure related to the armed conflict have also worked in favour of the Houthis in this regard. Because of disruptions to infrastructure and scarcities of fuel supplies, citizens' access to information was reduced largely to battery-operated radios, leaving mass media controlled by the very same group that implements strict information the primary source of news and information. Network traffic

monitoring data sources, such as those from Google and Dyn, help illuminate the timelines related to outages and, when used alongside corroborating information, can provide further precision to the analysis around attribution in future cases.

Our positive identification of the use of Netsweeper services in Yemen raises some serious concerns given that those services are being used to implement Internet filtering at the national level by a telecommunications ministry and an ISP controlled by the Houthis, the key leaders and allies of which have been sanctioned by the UN Security Council as a result of their activities exacerbating the conflict. The ongoing provision of services by Netsweeper to YemenNet, to control the flow of information amidst an armed conflict and under the direction of a group that has committed serious human rights violations against journalists and the media, warrants special scrutiny from a corporate social responsibility perspective. Netsweeper technology is being used to shape the information environment in the interests of one side of the armed conflict and is therefore implicated in a war-related information control machine that prevents citizens' right to know and media's right to inform.

We also find that the armed conflict in Yemen has international implications, as countries party to the conflict have implemented Internet censorship in their own jurisdictions, thus affecting their citizens' abilities to exercise their right to access information and communicate freely. Our network measurement tests show that Saudi Arabia has expanded its internet censorship practices to include content emanating from Houthi-owned and Houthi-controlled media and that which is critical of the Saudi-led military campaign, while Internet filtering in Iran blocks select Saudi and Yemeni media content, which bears similarities to that which we find in Yemen -- significant because the government of Iran is a principal supporter of the Houthis.

Lastly, the Yemen case study demonstrates how armed conflict can affect the information environment in surprising ways, but not in a vacuum. While the Houthis introduced radical measures that dramatically shifted access to information and means of communication, they did so on top of an existing technological infrastructure that included advanced content filtering systems provided by a company already contracted to the principal national ISP. Some reports, which we could not independently confirm, suggested they also inherited and are deploying advanced surveillance equipment. The Yemen case therefore underscores that "dual-use" technologies can be put to nefarious ends when circumstances change; and in situations of warfare, change can be extreme.

## Acknowledgements

---

The Citizen Lab would like to thank Doug Madory from Dyn for producing traffic and AS maps, Collin Anderson for collecting network measurement data and Masashi Crete-Nishihata and John Scott Railton for comments, and Irene Poetranto for layout. This research was supported by the International Development Research Centre (Canada) and the Social Sciences and Humanities Research Council of Canada (SSHRC) grant 430-2014-00183, Prof. Ronald J. Deibert, Principal Investigator.

## Data

---

A collection of data associated with this report, including lists of tested and blocked URLs, can be found at [Citizen Lab's Github repository](#).