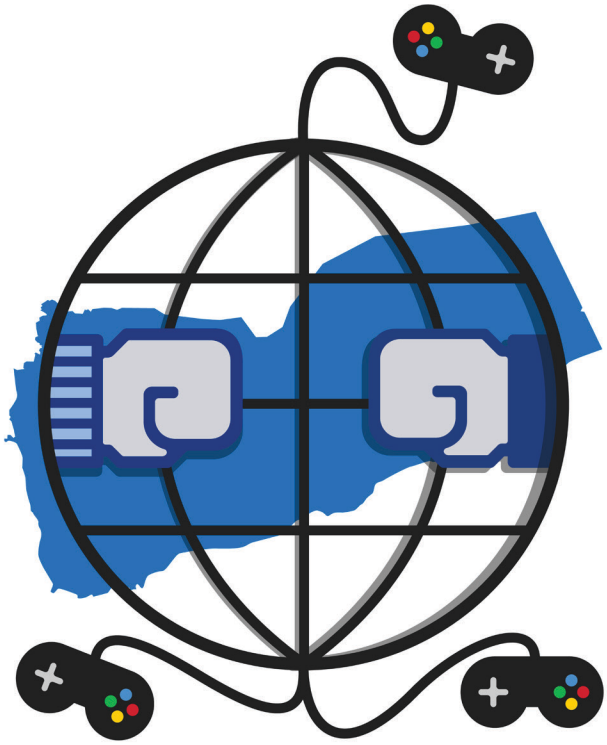
Recorded Future

CYBER THREAT ANALYSIS

Yemeni War Emphasizes Importance of Internet Control in Statecraft and Conflict

Emerging Trend of Internet Shutdowns in Venezuela, Bangladesh, India, and Sudan

By Insikt Group



CTA-2019-0312

This report serves as a follow up to Recorded Future's previous work, "Underlying Dimensions of Yemen's Civil War: Control of the Internet." It is intended to provide an update on previous reporting, as well as explore the trend of government-mandated internet shutdowns and access control.

Sources of this research include the Recorded Future® Platform, findings and methods from the Citizen Lab, Shodan, VirusTotal, Censys, GreyNoise, DomainTools, ReversingLabs, and third-party metadata. Recorded Future would like to thank the Citizen Lab, AccessNow, NetBlocks, Oracle/Dyn, and Freedom House for their continued reporting on internet outages, access restrictions, and censorship.

Executive Summary

Despite attempted peace talks in early December 2018, the conflict in Yemen has continued to claim lives. The World Health Organization declared the country in crisis after a rampant cholera outbreak that plunged the Arabian nation into a humanitarian disaster centered around an epidemic, a famine, and a civil war. A truce in the port town of Al-Hudaydah has not yet been broken, and may provide an avenue to deliver humanitarian aid to the country on the brink of starvation. Today, the grain stores held by the World Food Bank there are currently inaccessible, and may rot before a withdrawal is brokered.

As a result of continued airstrike activity, armed skirmishes among Yemeni factions, and the general degradation of Yemen's infrastructure and public health, the small amount of internet infrastructure in Yemen remains diminished. Despite indications of low usage, Recorded Future has observed an increase in the deployment of network control devices on YemenNet, the ISP controlled by Houthi forces. Recorded Future did not observe substantive changes on the Yemen top-level domain (TLD) space, or on either major internet service provider in Yemen.

Internet access control has become a growing trend, as internet disruptions, restrictions of information control, and other censorship methods have been increasing globally. Within Yemen, factions vie for control of internet infrastructure and use clever threat vectors in a few ways to control information entering and leaving their territories. The severing of or restrictions on internet use has become a norm in a wider trend of internet restrictions or blackout activity. India, Venezuela, Bangladesh, and Sudan have used diverse methods of controlling the internet access of their citizens.

Threat Analysis

Amid the fighting and the humanitarian disaster, international players still make attempts to leverage the horrible situation for positive headlines, or to maintain influence in Yemen. The United States stated that a January 6, 2019 drone strike against a known member of al-Qaeda in the Arabian Peninsula "delivered justice" in reprisal for the al-Qaeda bombing of the USS Cole in the Gulf of Aden in the year 2000. Saudi Arabian-backed missile strikes against the Houthi-held capital, Sana'a, continue to claim civilian lives despite being "targeted military strikes."

In February 2019, CNN published a report detailing how U.S.-made weapon systems originally sold to Saudi Arabia and the United Arab Emirates have allegedly reached the hands of al-Qaeda members and Houthi militias, including armored Mine-Resistant Ambush Protected (MRAP) vehicles. The Houthis, with the inadvertent aid of U.S. vehicles and weapons, have not only eclipsed a well-organized militia and become a more potent force, but have also become more capable of censorship and surveillance.

Recorded Future, via Shodan searches, identified the deployment of two additional Netsweeper devices on YemenNet on two IP addresses: 82.114.160.93 and 82.114.160.94. The device identified on 82.114.160.98 was still up at the time of this analysis. The re-emergence of censorship devices on the Houthi-controlled network may be a sign of momentary stability in Yemen's conflict, as operators may now have the time and safety to make the devices operational. Houthi forces have previously breached WhatsApp groups, and local contacts indicate that the group continues to have access to private chats, likely via individual mobile compromise or by enticing individuals to provide them data.

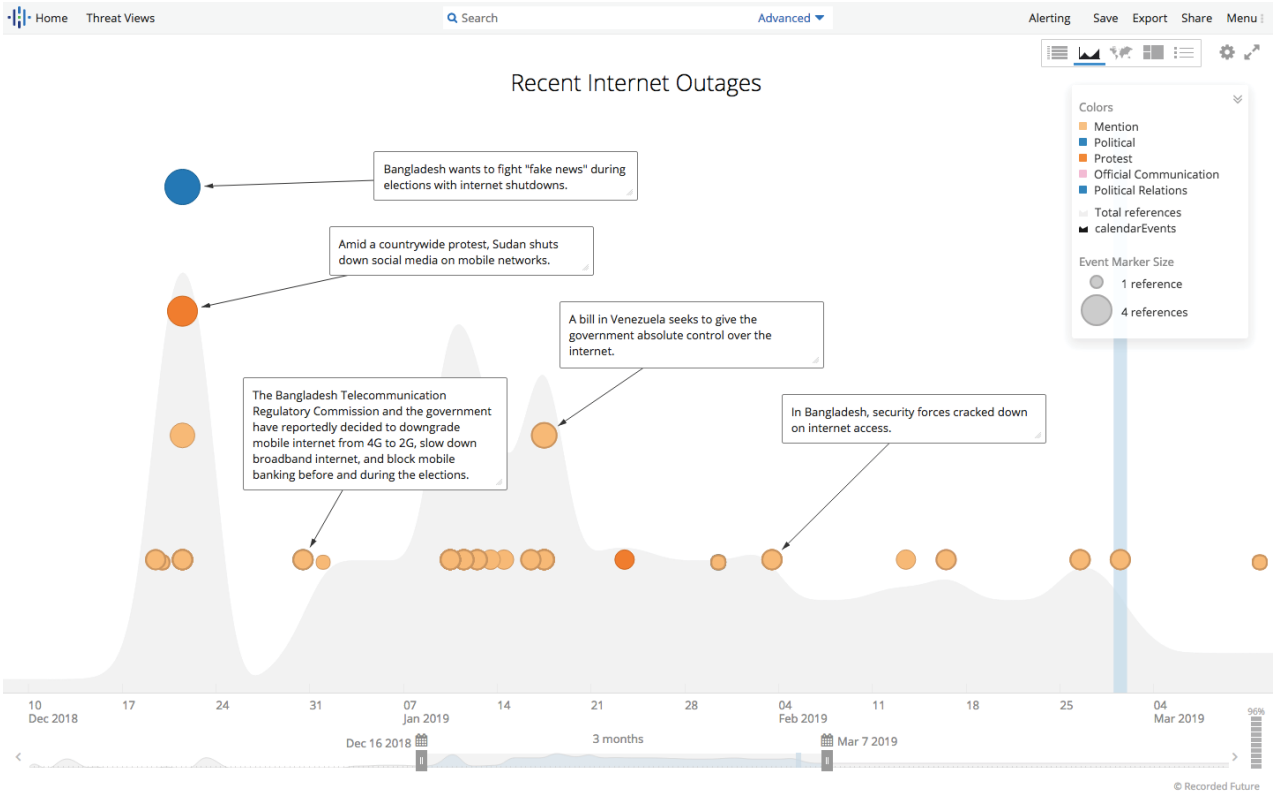
Recorded Future could not confirm the ongoing censorship of traffic in Yemen due to Netsweeper installations, which is likely a combination of low volumes of traffic in Yemen as well as a lack of monitoring capability and visibility within YemenNet. Rapid7's National Exposure Index found that although Yemeni ASNs have allocated 135,168 IP addresses, only 17,934 addresses were assigned, indicating low usage.

Recorded Future has not observed the widespread adoption of AdenNet in the country yet, which may be related to the fact that the Hadi government, which implemented the ISP, still resides largely in Saudi Arabia, and not in Aden. General internet usage appears low in Yemen, as GreyNoise data found only 538 total hosts observed in the country, which is a low number of hosts in a country of Yemen's size and IP allocation. Comparatively, Shodan detected a total of 44,451 devices in the country, but no data indicates that they are being used.

DomainTools data indicates that there are now 1,184 .ye domains (Yemen's TLD) — a minor increase of 32 domain purchases. Recorded Future did not observe any of these domain registrations. The TLD remains under the administration of the Houthis and YemenNet. This control of the TLD allows the Houthis to pose themselves as the legitimate administrators of Yemen to the outside internet.

Emerging Internet Disruption Activity Globally

The severing of undersea cables and other efforts to control Yemen's internet have not taken place in a vacuum, but rather have become a troubling trend globally, predominantly in Africa. Internet disruptions, information control, and other censorship methods have been increasing globally, according to a number of watchdog and non-profit organizations. Recent reporting has found that censorship of HTTP traffic, VPN blockages, and censorship of emojis happens in various nations. Of note, Venezuela, India, Bangladesh, and Sudan have used diverse methods of manipulating the internet access of their citizens.



Timeline of internet outages in 2019. (Source: Recorded Future)

These countries pose interest to multinational corporations for a number of reasons. Venezuela is a player in the international oil market, and the political situation there continues to destabilize international access to the country. Bangladesh is particularly interesting to retail companies, as a large proportion of the garment supply chain can be found in the the country. Finally, Sudan — and other African nations with lower rates of internet penetration — has been more inclined to shut down the internet in various ways and provide customers with interesting case studies in potential human rights abuses.

Venezuela

Venezuela has been immersed in political discontent driven by hyperinflation and shortages of food and medicine, heightened by power grabs, electrical instability, and internet outages. Rival factions have vied for power and control of Venezuela, with groups attempting to control internet and information access within the country. This has included small-scale, targeted DNS manipulation within Venezuela, country-wide blocking of streaming services, and total blackouts of any internet access.

Regional blackouts and country-wide internet disruptions have been reported in Venezuela since January 2019. NetBlocks has also reported on social media and information website blackouts inside of the country in relation to the disputed presidency and ongoing economic turmoil. NetBlocks further found an outage of YouTube, Periscope, and other streaming platforms during a speech from the interim president on January 27, 2019.

In February 2019, Kaspersky Lab found evidence of DNS manipulation within Venezuela. The attackers modified the DNS records of a legitimate volunteering website to a potentially malicious IP address in Venezuela which also hosted a malicious domain. This directed users inside of Venezuela to the malicious infrastructure while the rest of the globe was routed to the expected infrastructure. This activity is believed to be used to target and phish Venezuelan citizens who support interim president, Juan Guaidó, according to findings from Motherboard.

Bangladesh

On January 2, 2019, Bangladesh ordered a national-level throttling of all mobile data services in the country, ahead of its national election. Bangladesh chose to limit mobile data access, as 93 percent of the country's internet connections come from mobile phones, according to the Bangladesh Telecommunication Regulatory Commission. Recorded Future believes that these efforts are likely attempts to quell social unrest within the country to prevent the spread of information regarding the country's numerous accusations of human rights abuses.

The shutdowns appear to have the dual purpose of limiting communication within the country, as well as preventing the spread of evidence of atrocities within the country to the outside world. This appears to be similar to activity that Recorded Future observed in Yemen — with control of the internet infrastructure and Yemen TLD space, Houthi forces attempted to characterize Yemen as a Houthi country to the world outside. Recorded Future suspects that the Bangladeshi government may be attempting to control the external narrative of the country's internal affairs in a similar manner as exercised in Yemen.

India

India led the globe in 2018 in a number of internet disruptions and outages, with 134 reported incidents. The internet is so often disrupted in India that a service has been stood up to track the activity. The lack of connectivity in the country is not due to strained providers or insufficient infrastructure, but due to erratic, and sometimes unexplained government orders to fixed-line and wireless providers to revoke access. The incidents are described as "government-imposed disablement of access to the internet as a whole within one or more localities for any duration of time." The regularity of the activity is troubling, as is the scale of how much internet access is restricted or severed.

The majority of the shutdowns targeted mobile providers and have come from the northwest corner of the country, which borders regional rival Pakistan, including Punjab and Kashmir. The majority of shutdowns have come in response to reports of militant activity, and to quell potential rumors of further activity. Often, activity is degraded to 2G speeds, or entirely cut off, according to the Freedom House's 2018 report on internet freedoms in India. The report found that government officials often cite "precautionary measures" when ordering internet and cellular providers to reduce or shutdown access. Recorded Future anticipates that internet shutdowns in the border area will increase in scope and magnitude in the near term due to heightened tensions between Pakistan and India.

India's internet control differs from the others in scope, frequency, and methodology. India is a democracy, limiting internet access in minority regions to counterterrorism and militant activity. Typically, internet censorship and access control are associated with authoritarian regimes or developing nations, where India is a democracy and maintains the world's sixth largest gross domestic product value (GDP), a measure used to determine relative economic size. Researchers from Montclair State University estimated that the 59 internet blackouts in the border region in 2017 alone cost India nearly half a billion dollars in GDP.

Freedom House also published an annual report on global trends, which made note of countries globally purchasing Chinese telecommunications infrastructure, India being among those countries. Yemen, notably, has also purchased a large amount of equipment from Chinese telecommunication company Huawei. Alongside this infrastructure was the deployment of Netsweeper content filtering devices. Using Shodan, Recorded Future identified eight Netsweeper instances in the country, and found that five of those devices were signed with Huawei SSL certificates. Recorded Future could not confirm the ongoing censorship of traffic in India from the Netsweeper devices.

Sudan

Digital rights non-profits AccessNow and Netblocks reported a countrywide outage of access to Twitter, Facebook, Instagram, and WhatsApp across Sudan in December 2018. The blocking of those applications came amid protests following a 70 percent inflation and a spike of grain and oil prices in the country. Sudan's regime has responded harshly to the nationwide protests, cracking down on civilians with riot police using tear gas and live ammunition, killing dozens of protestors. Internet access was depreciated across the country, limiting access to the aforementioned applications to prevent "rumor mongering."

This censorship showed a coordinated effort across multiple ISPs to block access to social media and communication applications. Sudanese telecommunication providers Zain-SDN, Sudatel, and Kanartel were affected by the blackout, as was international telecom MTN, which reportedly did not block WhatsApp. This is likely indicative of the regime leaning on the internet service providers to facilitate an effective media blackout. Members of Anonymous encouraged Sudanese residents to use TOR or a VPN on their mobile devices to bypass the blockade, but there was no indication of whether this method effectively evaded the ISP blackout.

Methods of Internet Control in Statecraft and Conflict

These recent acts of censorship and internet shutdowns reflect different methods of internet access control regimes and rebel groups having to control information access. The more blunt methods generally lead to internet blackouts at large, as exhibited by Yemen when Houthi forces severed internet cables, as well as more brutish blackouts used by Bangladesh and Zimbabwe this year, subjecting citizens to total internet outages.

Countrywide censorship is also possible at the routing level, but is not always easily implemented. Russia made a failed attempt at blocking encrypted messaging application Telegram at the protocol level, and eventually blocked entire subnets belonging to Google and Amazon, which had widespread negative impacts on the country's internet. Turkey has used rough DNS hijacking against Google DNS and OpenDNS in 2014 to curtail the country's use of Twitter and other social media platforms. Iran has imposed content blackouts by using BGP hijacking to sinkhole media traffic, among other methods, including HTTP host–based blocking, keyword filtering, and protocol-based throttling.

Content-level censorship can be used in countries with large control of their IP and DNS infrastructure, as previously noted by Yemen's use of Netsweeper devices. The Citizen Lab has previously conducted research on these censorship devices, while new reports have found countries using technology capable of deep packet inspection for content monitoring in the Middle East.

Outlook

Censorship at these levels is not limited to the countries above, but internet control has become a tool being used more and more by countries as part of their statecraft. Government censorship is not a new trend, but outside parties are increasingly reporting on such incidents. States that implement such measures take a risk — they may maintain control over their populations, but these actions will also likely be detrimental to their domestic economies and stifle business opportunities. Countries that implement digital censorship tend to slow their own technological growth and business innovation.

These internet shutdowns can create heightened risk for the entire region they are affecting. Additionally, beyond the social costs, censorship and shutdowns can severely hamper economic growth and trade. Many businesses that operate online or rely on cellular service can incur heavy losses and can limit production in certain states. Corporations operating in those countries can lose control of their operations which can lead to tampering, or effectively have workers feel stranded without contact from their main headquarters.