Recorded Future

CYBER THREAT ANALYSIS

Underlying Dimensions of Yemen's Civil War: Control of the Internet

By Insikt Group
Recorded Future

CTA-2018-1128

Scope Note: Sources of this research include the Recorded Future platform, Recorded Future malware detonation, the findings and methods from the Citizen Lab, Shodan, VirusTotal, Censys, ReversingLabs, and third-party metadata. Recorded Future would like to thank Rapid7 and their National Exposure Index in helping quantify the current IP landscape in Yemen. Recorded Future would also like to thank Joe Security for the use of their product to analyze Android device malware samples.

Please see page 23 for a graphical representation of this analysis.

Executive Summary

In the midst of the ongoing Yemeni civil war, local and international players are waging a secondary war through internet control and other cyber means. Recorded Future's Insikt Group assesses that dynamics of the Yemeni civil war are manifesting themselves online through a struggle over Yemeni access, use, and control of the internet. Recorded Future identified both censorship controls and traffic attempting to subvert those controls within Yemen, as well as spyware activity. This report intends to establish a baseline of internet activity, use, and access in Yemen.

Key Judgments

- Since taking Yemen's capital, Sana'a, in September 2014, the Houthi rebels have supervised the main ISP YemenNet, as well as the same access controls and censorship tools previously used to disrupt, degrade, or monitor internet activity for the last three years.
- Recorded Future assesses with medium confidence that the Houthi rebels within Sana'a are taking advantage of YemenNet's vast IP infrastructure to host Coinhive mining services to generate revenue.
- While official government sites hosted on YemenNet and the .ye domain space have been changed to reflect the Houthi government in Sana'a, rather than the Hadi government in Aden, Recorded Future has noted some vulnerabilities within YemenNet's main name server and multiple servers that, until recently, hosted over 500 official .ye domains.

- The Hadi government, now in Aden instead of Sana'a, produced a new ISP, AdenNet, in June 2018. We believe this could lead to new internet resiliency within the country as internet subscriptions and mobile subscriptions continue to rise.
- A small percentage of internet users in Yemen are using either VPNs, Tor, or routers with DNS recursion to circumvent government controls.
- Suspicious internet-related activity out of Yemen suggests low levels of adware and spyware, but information as to the actors behind it is inconclusive.
- Major international players, including the United States, Russia, and China, are using malware, military activity, political leverage, and investments to further their interests in the Saudi-Iranian regional conflict for hegemony within Yemen.

Background

Yemen has been embroiled in an ongoing civil war since 2015. The conflict is fueled by sectarian, religious, and political divides, as Yemen is relatively multicultural compared to the rest of the Arabian Peninsula. The Yemenis have endured multiple civil wars, including a conflict in Northern Yemen from 1962 to 1970, and a bloody war in 1994 after resisting the country's 1990 unification. For all of its internal struggles, Ali Abdullah Saleh, a former president of Yemen, described governing the country as akin to "dancing on the heads of snakes."

The current civil war traces back to a series of bloody protests, spurred on by the Arab Spring, that caused President Ali Abdullah Saleh to resign from power in 2011. This placed the vice president, Abdrabbuh Mansur Hadi, in power in a difficult situation, mandated to form a unified government in Yemen. Hadi ultimately failed to unify the country, leaving it largely ungoverned. The lack of control led to a power vacuum that allowed the growth of rebellious factions, competing foreign-backed governments, and the festering issue of extremism.

The Zaidi Shia Houthis are largely considered to be the rebellious faction, and are backed and supplied by the Iranian regime. The faction was formed from members of Yemen's military previously loyal to Saleh before he turned on his own faction and was subsequently killed in 2017. The faction fights the Saudi-backed Abdrabbuh Mansur Hadi government, which currently claims political control of Yemen and is the internationally recognized government of Yemen. This fuels sectarian tensions, as the Hadi government supporters are largely Sunni Muslims, as opposed the Houthis, who are majority Shia. The United Arab Emirates funds a third group of southern separatists — a splinter group of the Southern Movement that has been actively trying to secede from Yemen since 2007. The group hopes to reestablish the borders from 1990, when the previously separate North Yemen and South Yemen were united to form one country. The Southern Movement is also predominantly Shia. These groups largely represent the different demographics within Yemen's borders.

Additionally, remnants of Al-Qaeda in the Arabian Peninsula (AQAP) continue to hold large pockets of territory in the center of the country. AQAP is one of Al-Qaeda's most prominent affiliates, taking credit for lone wolf attacks on Fort Hood, Little Rock, the USS Cole, and the failed airplane bombing in Detroit, as well as a jailbreak in Yemen. The group attempted a rebranding in 2011 as Ansar al-Sharia and began to focus on holding territory in Yemen. The group has predominantly operated as a militia and terror organization targeting Houthi installations in recent years. A similar affiliate model was attempted by the Islamic State, which largely failed to gain traction. The recent reporting of the Islamic State within Yemen surrounds skirmishes between AQAP and IS.

Yemen, as a battlefield, is an interesting microcosm of regional and global powers attempting to project their power and manifest their interests. The Yemeni civil war lies at the center of the Iranian and Saudi proxy battle for regional hegemony. Houthi-held territory has been targeted by Saudi Arabia's Operation Decisive Storm, an airstrike campaign which the United Nations claims continues to kill non-combatants. The Iranian campaign, according to the U.S. military, has introduced weapons that have allowed the Houthis to interdict shipping routes in the Bab al-Mandeb strait.

As tensions rise between the United States and Iran, Iran has the ability to control the Strait of Hormuz across the peninsula and has threatened a blockade if it perceives the United States has been too aggressive. Recorded Future has reported on Iran and Saudi Arabia's cyber conflict within Yemen previously in 2015, when the Yemen Cyber Army emerged as a patriotic hacking group attacking Saudi government agencies. The group has since been linked to Iran.

This regional conflict coincides with conflicting Russian and American interests in the Arabian Peninsula and the region's sea lanes. The United States has also led an active campaign to rid the region of the presence of the Islamic State (IS) and Al-Qaeda, finding success against IS but at the expense of civilian deaths in airstrikes and costly special operation campaigns. Conversely, the Jamestown Foundation has speculated that Russia has deployed private military contractors to Yemen to oversee a political solution to the war. The Carnegie Endowment believes that Russia is involved with the goal of expanding its influence and projecting power in the Red Sea.

China has also increased its interest in the stability of the peninsula and has aligned itself with the Hadi government and its Saudi-backed forces since approximately 2017. While China and the Saudi Arabian government have pre-existing defense ties, a resolution to the conflict in Yemen would help reduce the risk to Chinese shipping around the Bab al-Mandeb strait and the surrounding area. The strait is a key transit route for China's Belt and Road Initiative — a massive series of infrastructure projects designed to project Chinese national power — into Saudi Arabia and the wider Middle Eastern region.

Infrastructure

The internet infrastructure in Yemen is reflective of the international powers at play in the nation. The ongoing conflict has stunted the assignment of internet space, as well as the ability of citizens to access the internet. 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. According to DomainTools, there have only been 1152 .ye domains registered (.ye is controlled by YemenNet). People self-reporting as being from Yemen have registered 7,845 domains, the most popular of which is .com. The fourth most popular TLD is .ye. Yemen ranks 50th globally in population, but 148th in domain registrations.

As territory has changed hands in Yemen for the last four years, so too has control over internet resources. As the Houthi forces seized the capital city of Sana'a, they also gained control over YemenNet — the major internet provider to Yemen. YemenNet is prone to outages and was previously disrupted by both cyber and physical means.

Submarine Cables

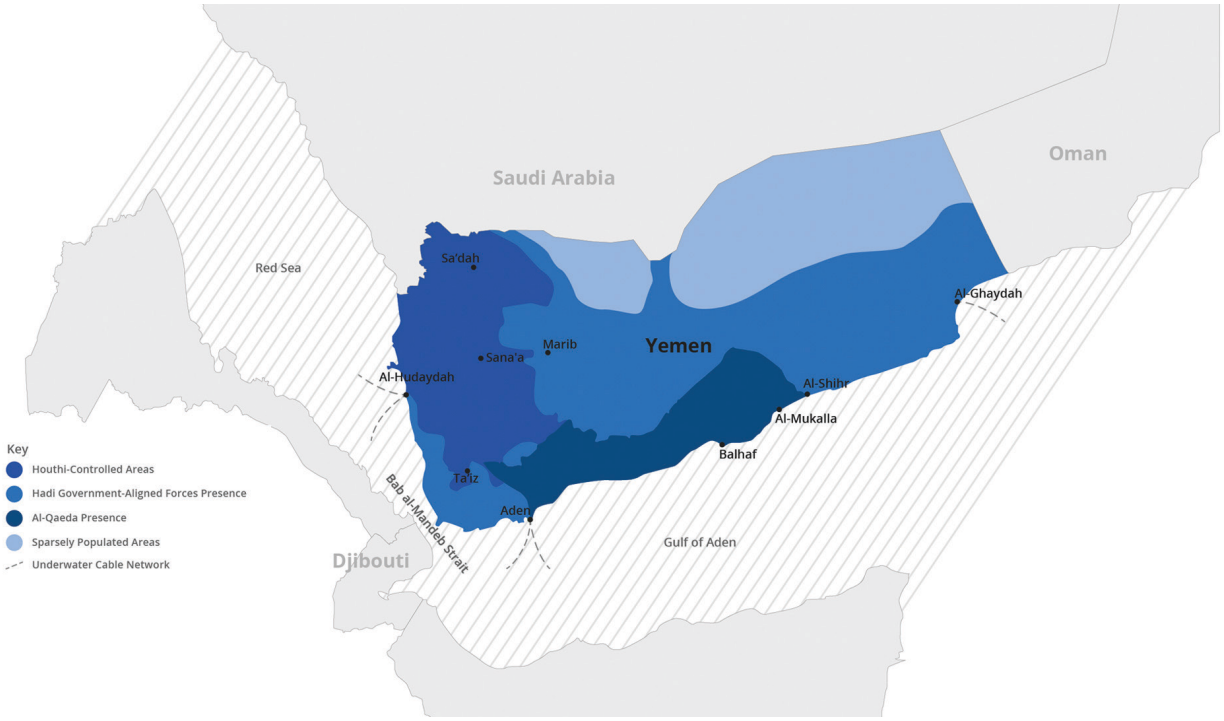
There are four submarine cables servicing Yemen at three landing points. As shown in the image below, the FALCON submarine cable has landing points at Al-Ghaydah and Al-Hudaydah, and SEA-ME-WE 5 also has a landing point at Al-Hudaydah, while AAE-1 and Aden-Djibouti have landing points at Aden.

Under Houthi control, TeleYemen (and therefore YemenNet) makes use of the submarine cables for routing traffic, most likely to avoid routing through the fiber-optic connections provided by Saudi Telecom. Currently, YemenNet peers with Reliance Globalcom, Cogent Communications, Omantel, and PCCW Global — all partners in the Asia Africa Europe-1 (AAE-1) submarine cable, which has a landing point in Aden. AdenNet, on the other hand, primarily makes use of the overland fiber-optic cables provided by Saudi Telecom.

Two of the three submarine landing points in Yemen are currently under the control of the Hadi government. The third, in Al-Hudaydah, is currently under the control of the Houthi rebels, but as shown in the image below, is an area that the Hadi government has been aggressively targeting. The port in Al-Hudaydah is critical for the delivery of food and medical supplies to a nation that is experiencing famine and a cholera outbreak. If the Hadi government forces take control of the port, they could cut off internet access between the outside world and YemenNet subscribers. While not as critical as the humanitarian crisis currently impacting Yemen, lack of internet access would make it more challenging to understand what is happening within the country.

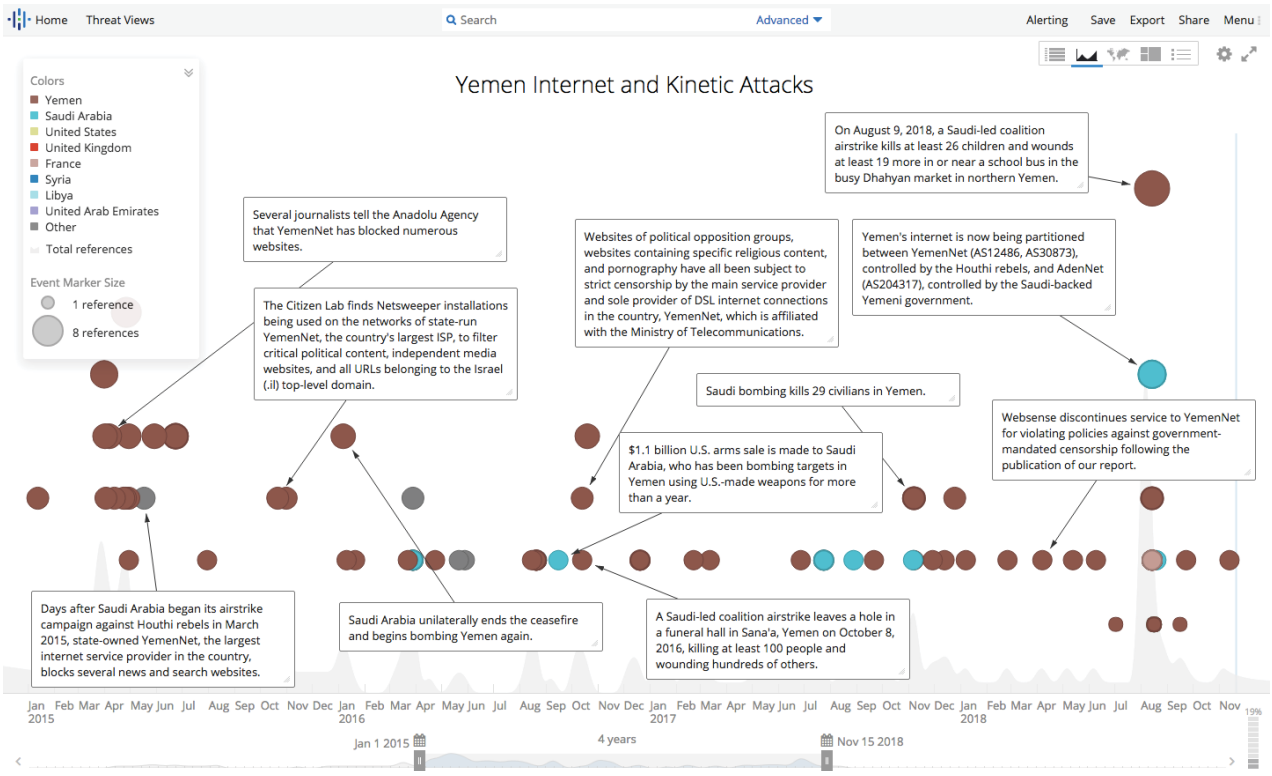
Access and Censorship

In 2015, the Citizen Lab reported that the Yemeni government was censoring content for Yemeni citizens on YemenNet, its only national ISP with control over the .ye namespace. Much of the IP and domain space used in YemenNet is filtered through two caching servers, cache0.yemen.net[.]ye and cache1.yemen.net[.]ye. This may allow for content monitoring or interdiction of traffic. Recorded Future found remnants of that effort via Shodan, with a single NetSweeper device, a tool for web content filtering, installed on the IP 82.114.160.98 (Intelligence Card). The IP used a self-signed SSL certificate, but Recorded Future could not identify any traffic going to or from that IP address. No other similar censorship or access control devices were found via Shodan or Censys.



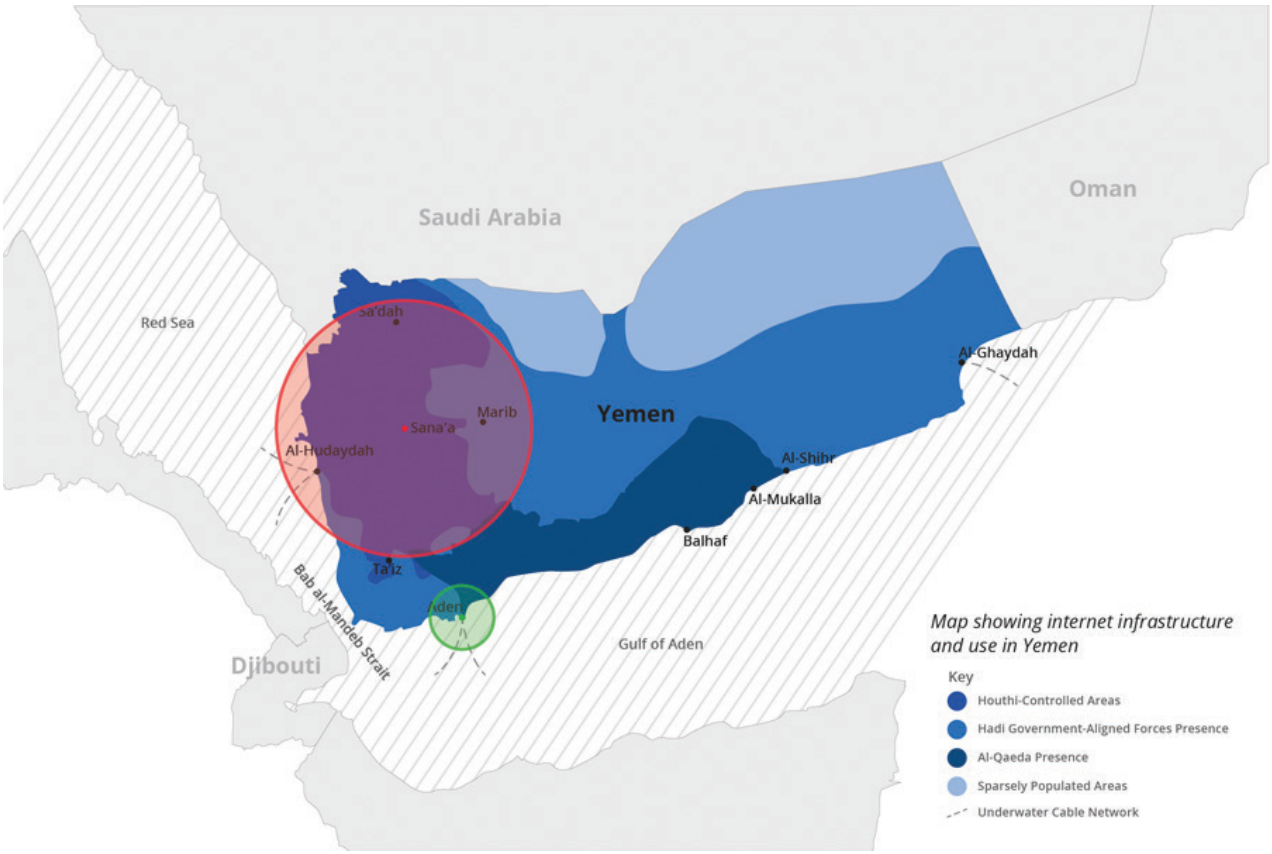
Geographic breakdown of internet access and territory control.
Source: Created from Al Jazeera, Reuters, World Energy Atlas, and Critical Threats (November 2018).

After taking over Yemen's capital Sana'a in September 2014, the Houthi rebels gained control over YemenNet, TeleYemen, and all other telecom providers based within the city. In June 2018, they also seized control of the dominant mobile provider, MTN Yemen. Thus, the Houthi rebels now have access to the same access control and censorship tools previously used to disrupt or monitor internet activity, which may come online or offline depending on the physical safety of operators using the boxes. The Houthis have used these to block access to WhatsApp, Facebook, Twitter, and Telegram, according to reports from Al Arabiya, along with domains that reported on Houthi troop movements. It is likely that they used these controls to do so.



Timeline of Yemeni internet activity and prominent airstrike operations.

The Houthis have also taken steps to shut off internet access entirely across their ISP control. On December 7, 2017, the Houthi-controlled Ministry of Communications and Information Technology initiated a shutdown of the internet for 30 minutes. Previously, the Houthis have disabled internet access to the port city of Aden. Numerous reports found that the Houthis severed over 80 percent of fiber optics lines from YemenNet, taking a more brutish approach to control information across the country.



Major internet service provider IP holdings.

Forced to flee the capital, the Hadi government established a base of operations in Aden. The new base also required internet access, and rather than seed secrets or money to the Houthi-controlled YemenNet or be at the mercy of the Houthi government repeatedly cutting off access, the Hadi regime stood up AdenNet, a new backbone provider, in June 2018. The new ISP was funded by the United Arab Emirates (UAE), uses a single flow from Saudi Telecom (AS39386), and was built using routers from Chinese technology firm Huawei. Huawei is a corporation with extremely close ties to the Chinese government and military and has been banned from government use in the United States and Australia due to espionage concerns.

Much of AdenNet's infrastructure is located outside of Yemen. The AdenNet website www.adennet4g[.]net was registered through GoDaddy on June 20, 2018, and is hosted at Bluehost, as is the AdenNet mail server (mail.adennet4g.net). Both hosts have the same IP address, 162.241.226.169, which according to Recorded Future research is shared by 886 other domains. Customer service functions, such as the self-service portal ssp.adennet4g[.]net, do make use of assigned AdenNet IP space.

The use of the .net gTLD for AdenNet and outside infrastructure may reflect the reluctance of the Hadi regime to use Houthi-controlled resources. It could also be indicative of the challenges that come with trying to build out new internet infrastructure, especially in the middle of a war zone. Earlier reports suggested that President Hadi is attempting to regain control of the .ye ccTLD, as well as the AS30873 and AS12486 ASNs. A review of documents at ICANN, IANA, and RIPE indicate that, as of this report, no formal process has been started. In addition, the likelihood of control of these resources being transferred by internet-governing bodies in the middle of a civil war is very low.

Baselining Internet Activity

Airstrikes and food shortages during the Yemeni civil war have left 18 million people in need of humanitarian assistance and have created a food emergency. However, internet activity from the country has not decreased during the war. According to the CIA World Factbook, internet users have risen from 19.1 percent of the population before the war in 2014 to 24.6 percent in 2016. Internet World Stats also claims that internet users have stayed roughly the same over the past two years, hovering at 24.3 percent in 2018. Additionally, multiple sources claim that cell phone penetration has been above 50 percent since before the country's civil war and has either stayed roughly the same or grown over the last four years.

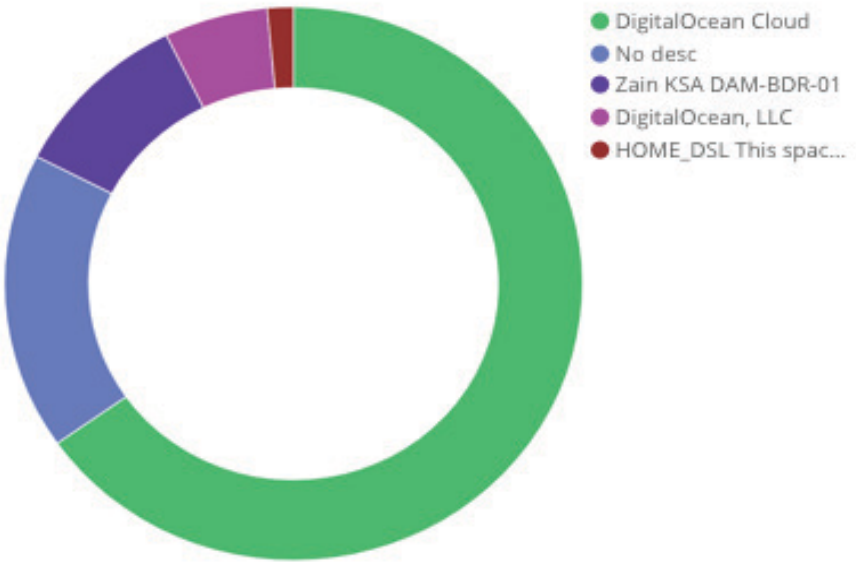
There is evidence of five different forms of users utilizing internet services within Yemen. The Houthi rebels used their control of YemenNet and the .ye domain space after taking Sana'a, and government websites reflect the current Houthi government within the capital. For example, the website of Yemen's Ministry of Foreign Affairs contains an up-to-date list on the current Houthi-led ministry. Additionally, with the creation of AdenNet, the Hadi government will likely be using internet services more frequently.

Screenshot of Yemen's Houthi-led Ministry of Foreign Affairs website under the domain mofa.gov[.]ye.

Universities also still have access to the internet within the country, and university students are still using internet services to conduct research, communicate with each other, and browse the web. However, this is becoming an increasingly smaller source of traffic as universities are gradually being targeted in airstrikes and bombing attacks by both Houthi and Hadi-led factions, causing university enrollment to decrease. Additionally, universities in the country are increasingly being repurposed as detention centers, which is likely another reason for a drop in university internet usage.

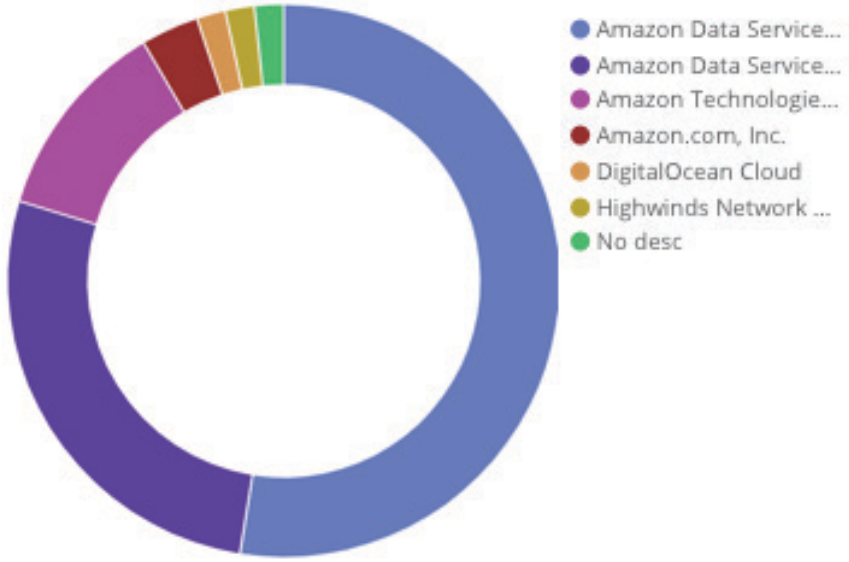
A disproportionately large number of home and business users in Yemen have enabled DNS recursion on their routers, which allows these routers to act as a caching DNS server for the users behind the router. According to Shodan, there are more than 12,000 customer premise equipment (CPE) routers with DNS recursion enabled. It is possible that this is being done to bypass the reported draconian censorship enforced by the Houthis — as mentioned earlier, they are reportedly using Netsweeper, a tool that uses a combination of web and DNS filtering, to block content deemed objectionable.

For comparison, the countries of Mozambique and Ghana, which have similar population sizes to Yemen, only report around 670 and 1200 open DNS servers in Shodan, respectively.



Breakdown of Yemeni traffic destinations to OpenVPN endpoints, according to third-party metadata.

Finally, multiple sources have suggested that Yemeni citizens have used either Tor Browser or VPNs to get around Yemeni internet shutdowns and censorship. This user group would likely be accessing sources that are not sanctioned by either the Houthi-led rebels (who temporarily shut down the internet across the entire country on December 7, 2017) or the Hadi government, which has a history of blocking various social media outlets. Recorded Future found evidence of VPN and Tor usage from Yemen during October 2018. Small amounts of traffic from multiple AdenNet IPs were attempting to access non-Yemeni IPs that had open ports 9001 (Tor), 1194 (OpenVPN), or 110 (IPSEC VPN tunneling).



Breakdown of Yemeni traffic destinations to Tor endpoints, according to third-party metadata.

Quantifying Internet Use in Hadi-Controlled Yemen

AdenNet is much smaller than the now Houthi-controlled YemenNet. To assess the types of traffic that were coming from the ISP, Recorded Future conducted metadata analysis from October 1, 2018, to November 6, 2018. Recorded Future chose to monitor AdenNet because of its recent creation, and because it is under the control of the Hadi government, making the analysis of this ISP useful to gain insight into what is occurring in Hadi-controlled Yemen. Although most major cities within Yemen have been hit by bombings since the creation of AdenNet in June 2018, both YemenNet and AdenNet seem to be functioning without much issue, based on traffic between the two ISPs and the publicly known YemenNet hosts online.

Recorded Future map of airstrikes or bombings in Yemen since June 2018.

Top Ports and Protocols: Web Browsing and VPNs

Most of the activity we observed during our analysis of the Yemeni internet, somewhat unsurprisingly, was web browsing activity over HTTP or HTTPS. In addition, we also identified sporadic DNS, POP3, SMTP, and IMAP activity. We observed some IPSEC tunneling activity utilizing the Encapsulating Security Payload (ESP) protocol, which is indicative of VPN application use. This could be further evidence of Yemeni users attempting to circumvent either government's internet controls in order to get online. Other activity included the use of internet administrative protocols TELNET, SSH, and the network news transfer protocol (NNTP), one of the internet's oldest protocols, allowing for news article transfer between servers of the internet USENET newsgroup world. Finally, evidence of BitTorrent and online gaming activity as well as the possible use of XMPP messaging applications such as Jabber were also found.

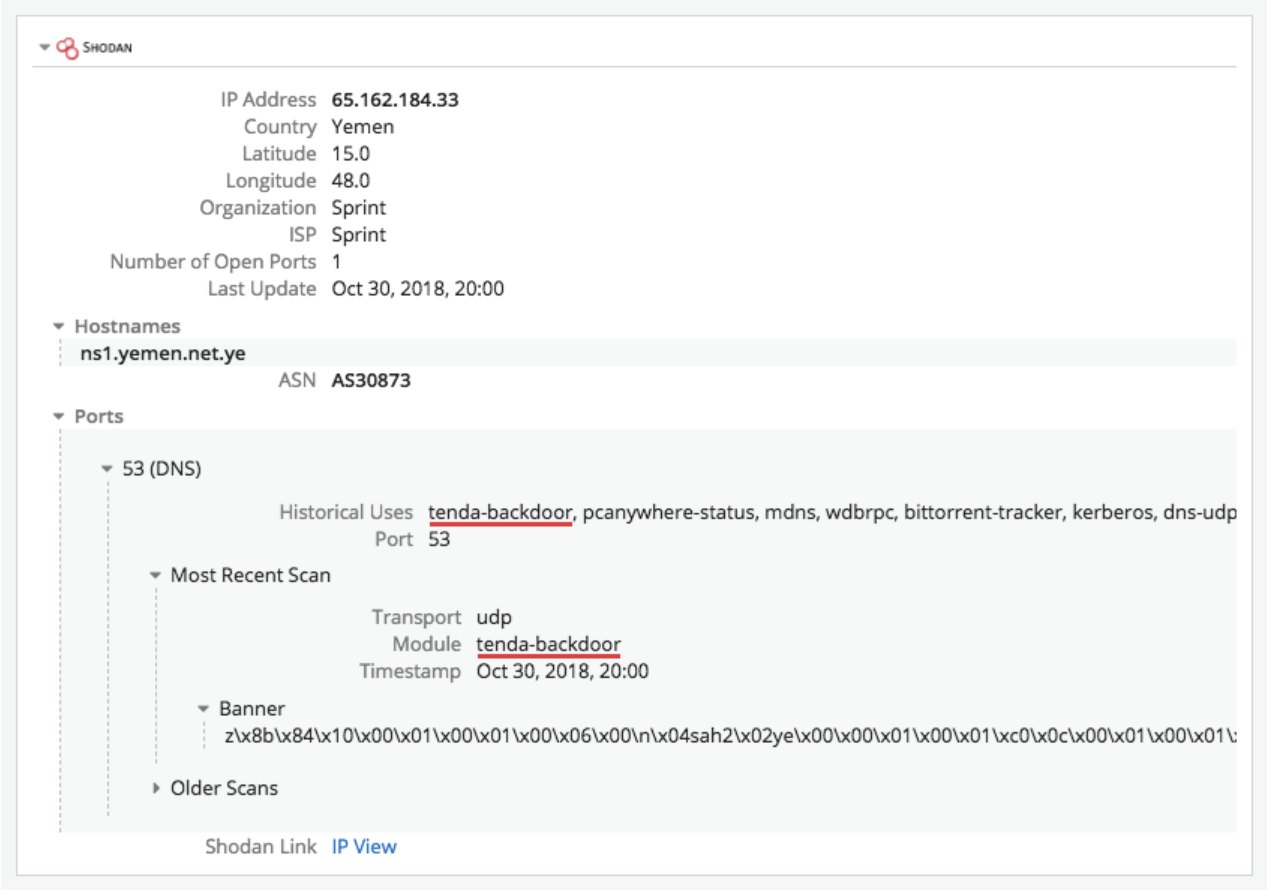
Because most of the traffic we observed was web browsing activity, it is no surprise that most traffic originating from AdenNet IPs within the Recorded Future dataset were headed toward large hosting sites and content distribution network (CDN) providers like Highwinds, Amazon, and Akamai. What is surprising is the distribution between Western and Chinese-owned hosts. Alibaba and Tencent hosting services, while not as frequently accessed as their western counterparts, still show up as a sizable percentage of Yemeni internet traffic.

Suspicious Internet Activity

Internet Infrastructure Vulnerabilities

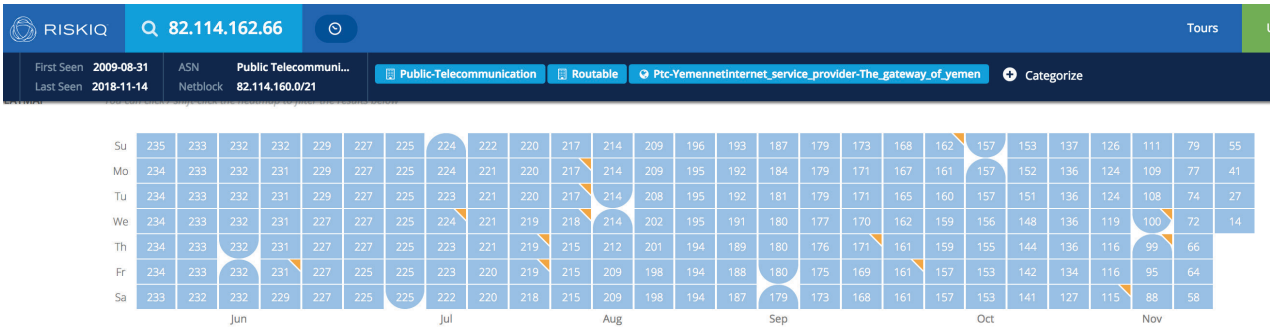
Recorded Future has found multiple instances of suspicious activity within and originating from Yemen's internet infrastructure. For one, AdenNet does not seem to be the first time that Yemen has entrusted a Chinese company with its backbone internet infrastructure. Recorded Future's Shodan integration shows that the IP for one of the main nameservers in YemenNet, ns1.yemen.net[.]ye, contains a "tenda-backdoor" module. While this module is no longer searchable in Shodan, the tenda-backdoor module refers to a firmware backdoor using vulnerability CVE-2017-16923 to conduct remote command execution in router models made by Chinese network manufacturer Tenda.

It is uncertain whether or not this was an intentional vendor backdoor or an accidental one. If the name server is connected to other infrastructure within YemenNet, which it is likely to be, both state and non-state attackers could leverage this backdoor to infiltrate the ISP.



Screenshot of the Recorded Future Shodan extension for ns1.yemen.net[.]ye.

Additionally, Houthi-controlled servers 82.114.162.66 and 82.114.162.10 that, up until June 2018, hosted upwards of 500 Yemeni government, educational, and corporate websites, are riddled with old vulnerabilities like CVE-2003-1582, CVE-2009-2521, CVE-2008-1446, and other older issues that, if left unpatched, could allow attackers easy access into said systems. Even though many of the original websites are no longer hosted on these servers, it is entirely possible that old system logs and data remain.



Screenshot of PassiveTotal domain results for the IP 82.114.162[.]66 on given days in 2018.
Source: PassiveTotal.

Command and Control Servers

Recorded Future's collections, in conjunction with Shodan, identified a number of basic command and control servers exposed in Yemeni ranges running remote access trojans. These included the Bozok, DarkComet, and NetBus trojans.

Malware Samples

Recorded Future noted a significant increase in the number of software samples submitted to VirusTotal from Yemen, from 13 samples from between 2015 and 2017 to a total of 164 samples in 2018. The cause remains unclear. This may be due to the introduction of AdenNet, as internet access becomes more consistently available to more citizens and residents of Yemen; however, it may also be due to increased threat activity.

Of these samples, approximately half were malicious, and the overwhelming majority of those malicious samples were Android applications. From the 84 Android samples uploaded to VirusTotal since 2015, Recorded Future was able to use Joe Security to identify variants of widely disseminated malware families, including AhMyth, DroidJack, Hiddad, and Dianjin, as well as multiple fake Altcoin wallets, fake Whatsapp applications, and spyware posing as antivirus, video playing, and VPN applications. In addition, Recorded Future used Joe Security dynamic analysis and Recorded Future malware detonation to determine that 50 percent of the adware obtained from the Android samples reached out to both Chinese and Western advertisement sites. Two-thirds of the fake antivirus spyware apps, as well as some AhMyth samples found, connected to Chinese IPs.

Most applications within the VirusTotal dataset appear to be low-level fake applications serving adware. However, some spyware from the dataset has been packed with JiaGuBao, a commercial packer from China. Additionally, the fake antivirus spyware reaching out to Chinese IPs accesses information from Android phones including old emails, SMS and call logs, and browser history. It likely uses accessibility services to control other installed applications and has the capability to change Wi-Fi configuration, start services while the phone screen is off, take photos, and delete other packages. There is no doubt that China is interested in the outcome of the civil war in Yemen both from a commercial and diplomatic perspective. However, while some of the malware reaching out to Chinese IPs align with possible Chinese surveillance interests, Recorded Future was unable to determine whether any malware obtained was from a Chinese nation-state espionage campaign. In addition, Recorded Future uncovered several Chinese mobile apps that requested extensive Android phone permissions being used by individuals in Yemen. Because these applications are currently only available on Chinese app stores, it is unlikely that the apps were being used by native Yemenis, but rather, Yemen-based Chinese nationals likely stationed in Yemen for capacity building purposes. Chinese companies, including Huawei, have sent Chinese workers to foreign countries in the past when constructing infrastructure projects. Chinese nationals would likely download applications tailored to them while in Yemen.

Coin Mining Activity

Recorded Future found 973 hosts within Yemen running cryptocurrency mining service Coinhive. Coinhive, a JavaScript-based Monero miner, was released in early 2017, two years after the Houthi rebels took control of YemenNet. It is usually embedded into websites and utilizes a user's CPU or processing power to mine cryptocurrency for the benefit of the website's owner. This will often lock a user's browser and drain the user's device battery for as long as they are browsing the site. All 973 hosts are MikroTik routers belonging to the YemenNet ASN AS30873, and 213 of the hosts share the same domain, dynamic.yemennet[.]ye.

In October 2018, Avast released a report of multiple cryptojacking campaigns in which attackers were using a widely available exploit[1] leveraging CVE-2018-14847 and injecting the required JavaScript code to run Coinhive on the compromised routers. Recorded Future found Monero miners using the unique SSH and Telnet ports mentioned by Avast, and determined that approximately 427 out of the 973 routers were involved with previous, more widely targeted campaigns already mentioned in Avast's reporting. The other 546 routers have thus far been left without any link to previous campaigns. A third of the unaccounted hosts (189) are located in Sana'a, the Houthi-held capital. "Unique" site keys generated by Coinhive admin accounts have been reused for multiple hosts, suggesting that a few accounts control a large majority of these hosts.

Additionally, all of the infected routers are part of the YemenNet network, while identical MikroTik routers owned by TeleYemen have not been infected. We were unable to determine who was responsible for infecting these YemenNet routers or why TeleYemen routers were also not victimized. However, available data leads us to three possible scenarios:

1. The TeleYemen hosts could be part of another criminal Coinhive campaign, due to partial overlap in Coinhive keys with previously discovered non-Yemeni hosts mentioned in the Avast report.
2. Parties interested in degrading the capacity of Houthi internet services during airstrikes or other conventional battles could be using the available Coinhive exploit to slow down YemenNet's machines, which would restrict government communications and civilian online services and even take hosts offline.
3. The Houthi-led government could be attempting to use their own hosts to generate alt-currency for the regime. Additional sources of revenue during a time of famine and economic crisis would bolster Houthi-led efforts to legitimize themselves domestically by providing aid to Houthi regions where famine is harshest and purchasing additional conventional weapons to use against the Hadi-led government.

[1] https://www[.]github[.]com/BasuCert/WinboxPoC

Regardless of the actors involved, we assess that the current coin mining campaign is draining Houthi-held internet resources. The Monero mining algorithm is specifically designed such that ordinary computers could generate the cryptocurrency as easily as computers with custom-made mining chips (ASICs). This is the opposite for Bitcoin mining, in which the mining power of ASICs render standard PCs ineffective. Recorded Future was unable to determine how much Monero has been generated from these efforts.

Expected Cyber Targeting Profiles

Recorded Future expected certain targeting profiles for each of the major belligerents in the Yemen conflict. This section will explore that expected activity, along with any differences or lack of data affecting those parties.

Houthi Supreme Political Council

The fact that the Houthis control a vast amount of internet resources in Yemen, are supported by Iran, and exert de facto control over the country continues to antagonize the Saudi Arabian government. This likely makes them the target of Saudi Arabian surveillance. Recorded Future expects this surveillance would be primarily used to identify Houthi intent and battle plans for skirmishes across Yemen, and would target routers, traditional hosts, and Android mobile devices. The Citizen Lab tied the Saudi's use of the NSO Group's Pegasus espionage tools to target iOS devices, showing the Kingdom's relative intent to outsource the development of their malware.

Lookout found that the NSO Group's spyware for Android devices, Chrysaor, uses Message Queue Telemetry Transport (MQTT) for communications. The protocol uses TCP/IP port 1883 and port 8883 when traffic is encrypted over SSL. This protocol is also used by the common MeetMe social media platform and is commonly used for connections in remote locations that do not always have uptime. Despite Houthi control of YemenNet, Recorded Future could not identify any infections using the conventional Chrysaor configuration in YemenNet or in any of its collections.

Hadi Government

The Hadi government is directly supported by Saudi Arabia, attempting to bolster Sunni and Saudi influence in their neighboring country, and are direct combatants with the Iranian-backed Houthi forces. Recorded Future would anticipate, due to the Hadi government's cooperation with China, that there would be some Chinese monitoring of Yemeni activity, even just as a manner of monitoring their investment. Additionally, Recorded Future would expect Iranian mobile surveillance malware deployed against these forces, which CheckPoint found to be used against Iranian dissident civilians and potential Islamic State sympathizers.

Southern Secessionists

The Southern Movement, formally known as the Southern Transitional Council (STC), is largely backed by the United Arab Emirates, but has found itself in an uneasy alignment with the Saudi coalition, which has often been tested and broken. In October 2018, the STC forces called for an uprising in Aden, directly conflicting with the Hadi government's control of the city. The activity provoked further UN calls for peace, allowing the group to gain more international recognition for their goal of an autonomous South Yemen. Due to the UAE and Saudi governments' cooperation and general alliance, Recorded Future does not anticipate Saudi targeting of the STC forces. Similarly, although the STC is in direct conflict with the Houthis, due to their lack of continued internet holdings or defined cell ranges, Recorded Future does not anticipate any particular targeting by Iranian malware against the STC.

Al-Qaeda in the Arabian Peninsula

Al-Qaeda's affiliate in Yemen is surprisingly in a peculiar targeting scenario. The group largely has the backing of the Saudi-led coalition, according to the Carnegie Endowment, sharing a common goal of fighting the Houthis. The Saudis even signed a nonaggression pact with the extremists. This conflicts with the U.S. backing of Saudi Arabian interests, as the United States is largely targeting AQAP forces almost exclusively in Yemen. The Iranians likely oppose the targeting of Houthi forces by the Saudi-aligned extremists.

Kaspersky found the Slingshot framework targeting individual routers in Yemen and other nations from 2012 to 2018. Slingshot was said to be used by the United States military to target Islamic State and Al-Qaeda members, perhaps in the most publicized instance of cyber being used for terrorist monitoring. Recorded Future could not identify any of this activity.

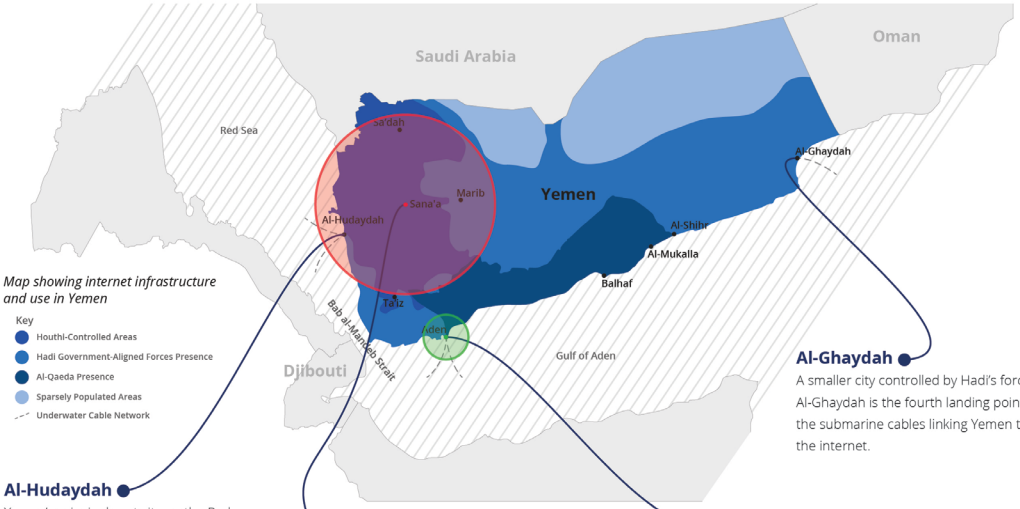
Outlook

Despite the continued airstrike activity, armed skirmishes among Yemeni factions, and general degradation of Yemen's infrastructure and public health, internet access in Yemen may prove to be resilient. The introduction of AdenNet to create a dual backbone in Yemen has created an additional network access point to thousands of citizens who had their internet access revoked when the Houthis seized Sana'a. However, vulnerabilities within YemenNet may lead to espionage or even destructive campaigns within its infrastructure, damaging internet access within Houthi-controlled territory.

Recorded Future assesses with medium confidence that, as inflation grows more rampant within the country, the Houthi government in Sana'a will continue its attempt to generate alternate forms of currency to bolster their aid and military efforts. Malware within the country will continue to be a constant factor, especially with new forms of access to the internet. Similarly, some Yemeni citizens will likely continue to circumvent government internet controls, understanding both governments' desire to control internet access in the past. Unfortunately, access to information or cyber means will likely not help bring Yemen back from the brink of famine, a Cholera outbreak, or the atrocities of continued civil war.

What's at Stake: The Underlying Dimensions of Yemen's Civil War

In the midst of the ongoing Yemeni civil war, local and international players are waging a secondary war through internet control and other cyber means. Recorded Future's Insikt Group assesses that dynamics of the Yemeni civil war are manifesting themselves online through a struggle over Yemeni access, use, and control of the internet.



Map showing internet infrastructure and use in Yemen

Key
- Houthi-Controlled Areas
- Hadi Government-Aligned Forces Presence
- Al-Qaeda Presence
- Sparsely Populated Areas
- Underwater Cable Network

Al-Hudaydah

Yemen's principal port city on the Red Sea, Al-Hudaydah, occupies a position of strategic importance. Four submarine cables link Yemen to the internet across three landing points, and two terminate at Al-Hudaydah, which is currently controlled by the Houthis but heavily contested by Hadi's forces. Two landing points are in Aden — if the Hadi government recaptures Al-Hudaydah, they will completely control Yemen's internet access points.

Sana'a

Once the capital of Yemen, Sana'a is now under Houthi control. Most of the country's internet infrastructure is in Sana'a — by capturing the city, the Houthis now control YemenNet, the country's main ISP. The Houthis heavily censor and restrict internet access over YemenNet through both cyber and physical means. They are also mining cryptocurrency using Coinhive.

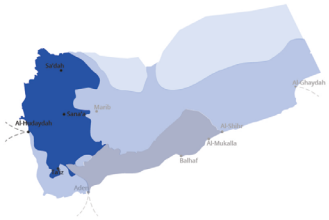
Aden

Aden is now the seat of the Hadi government and the internationally recognized capital of Yemen. In June 2018, the government developed AdenNet, their own ISP, which was funded by the UAE, uses a single flow from Saudi Telecom, and was built using routers from Huawei, a Chinese technology firm.

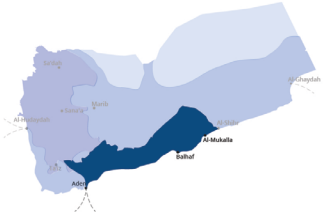
Al-Ghaydah

A smaller city controlled by Hadi's forces, Al-Ghaydah is the fourth landing point for the submarine cables linking Yemen to the internet.

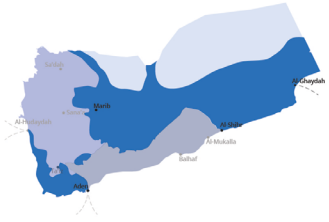
After the Arab Spring in 2011, the political factions in Yemen failed to agree on the future of the country's governance, creating a power vacuum and fracturing the country.



The Houthi movement — A faction of mostly Zaidi Shia Muslims, the Houthis reject the legitimacy of Hadi's government. The civil war began in 2015 after they captured Sana'a and territory in northern Yemen. The Houthis are supported by Iran, which seeks to increase its influence in the region.



Southern separatist movement — The United Arab Emirates (UAE), despite being part of the Saudi-led coalition that supports Hadi's forces, also funds separatists in the south who hope to reestablish the borders from 1990, when the country was separated into North Yemen and South Yemen.



Hadi's government — Abdrabbuh Mansur Hadi has been Yemen's president since 2012. After Houthis captured Sana'a, Hadi's forces moved to Aden. Hadi's government is supported by Saudi Arabia, which seeks to prevent Iran's influence in the region from growing. Most of Hadi's forces are Sunni Muslims.

Terrorist organizations — Al-Qaeda in the Arabian Peninsula (AQAP) and the Islamic State maintain nominal control of parts of Yemen, particularly in the south and east of the country.

Other international influence — The United States, Russia, and China also have vested interests in Yemen. The United States has worked to defeat the Islamic State and Al-Qaeda in Yemen, and Russia has possibly deployed private military contractors to Yemen to expand its influence and projecting power in the Red Sea. China has lately aligned itself with the Hadi government — ending the conflict would reduce the risk to Chinese shipping around the Bab al-Mandeb strait, a key transit route for China's Belt and Road Initiative.

Recorded Future

www.recordedfuture.com
@RecordedFuture