LILY HAY NEWMAN SECURITY 11.17.2019 03:34 PM

How the Iranian Government Shut Off the Internet

After years of centralizing internet control, Iran pulled the plug on connectivity for nearly all of its citizens.

PHOTOGRAPH: AFP/GETTY IMAGES

Amid widespread demonstrations over rising gasoline prices, Iranians began experiencing internet slowdowns over the past few days that became a near-total internet and mobile data blackout on Saturday. The government is apparently seeking to silence protesters and quell unrest. So how does a country like Iran switch off internet access to a population of more than 80 million? It's not an easy thing to do.

Though some countries, namely China, architected their internet infrastructure from the start with government control in mind, most don't have a central set of levers they can pull to influence countrywide access to content or connectivity. But regimes around

the world, including those in Russia and Iran, have increasingly been retrofitting traditional private and decentralized networks with cooperation agreements, technical implants, or a combination to give officials more influence. In countries like Ethiopia, Venezuela, and Iraq, along with disputed regions like Kashmir, government-led social media blocking and more extensive outages have become the norm.

“This is the most wide-scale internet shutdown that we’ve seen in Iran,” says Adrian Shahbaz, research director at the pro-democracy group Freedom House, which tracks internet censorship and restriction worldwide. “It’s surprising to see the Iranian authorities block all internet connections rather than only international internet connections, because the latter is a tactic that they’ve used in the past. It could mean they are more fearful of their own people and worry that they cannot control the information space amidst these economic protests.”

The process to block an entire country's internet connectivity depends on the set-up. Places like Ethiopia that have relatively limited internet proliferation typically have just one government-controlled internet service provider, perhaps alongside some smaller private ISPs. But all usually gain access from a single undersea cable or international network node, creating upstream choke points that officials can use to essentially block a country's connectivity at its source.

The more extensive and diverse a country's infrastructure, though, the more involved the digital blackout process becomes. Alp Toker, the director of nonpartisan connectivity tracking group NetBlocks, says it took Iranian authorities about 24 hours to completely block the nation's inbound and outbound traffic—leaving it hovering at about 5 to 7 percent of typical connectivity levels. Top politicians, like the country's supreme leader, Seyed Ali Khamenei, have still been using Twitter and other public platforms.

> **"The more networks and connections a country has, the more difficult it is to cut access for good."**
>
> – SECURITY RESEARCHER LUKASZ OLEJNIK

In a country without one or two obvious digital bottlenecks, authorities must coordinate with multiple telecoms, including ISPs and mobile data providers, to cut access. And they also need to overcome redundancies and algorithmic protections meant to make networks resilient in case of unintentional outages or bugs. For example, the internet is designed with failsafe properties that allow it to sort of quarantine and route around areas of a network that are suffering connectivity issues or other instability. NetBlocks' Toker says that perhaps Iran's internet slowdowns in the lead-up to the full outage were the result of telecoms working on behalf of the government to essentially defeat their own system reliability protections.

"To shut down a country's access to internet, it takes a lot of preparations. We are talking about software and hardware layers, and also regulatory frameworks," says Lukasz Olejnik, an independent security and privacy adviser and research associate at the Center for Technology and Global Affairs at Oxford University. "The more networks and connections a country has, the more difficult it is to cut access for good. And the question also is whether you want to cut in-country network access, too, in addition to flows between the country and outside world."

Increasingly over the past decade, the Iranian regime has focused on building out a centralized national "intranet." That allows it to provide citizens with web services while policing all content on the network and limiting information from external sources. Known as the "National information network" or SHOMA, the effort has centered on the state-owned Telecommunication Company of Iran, which is run by a number of former government officials. In the process of establishing this internal web, the Iranian regime has taken more and more control over both public and private connectivity in the name of national security.

That means Iran is also able to exert pressure even on ostensibly

independent internet providers. NetBlocks' Toker points out, for example, that his organization saw three Iranian mobile data carriers shut off seemingly in unison on Saturday. Still, he and other analysts emphasize that it's difficult to know exactly what has happened or why Iran's networks are specifically designed the way they are.

"In Iran, convincing operators probably isn't the most challenging task, because all of this has been normalized to a certain degree," says Toker. "But there's no indication of a national kill switch in this case. Around the world it seems like there's a sort of playbook that's developing, though."

That playbook chiefly involves the ability, one way or the other, to send the command for ISPs to shut it all down. It's a more involved request than blocking a specific platform like Twitter, another popular approach among Iran and other oppressive governments. That takes selective filtering rather than a near-total blackout. As of Sunday evening local time, Iran's internet was still down.

> **"It's not going to work. Information is going to continue to spread by other means."**
>
> — ADRIAN SHAHBAZ, FREEDOM HOUSE

The United Nations has explicitly identified government-led internet shutdowns and censorship as a human rights violation. But numerous governments have been pushing the limits of how much they can

curtail connectivity without facing reprisals from the international community. And just this week, United States UN representatives and others warned that a Russian-led cybercrime resolution that will face a UN vote Monday is really a treaty that could be interpreted to allow government internet control. Even countries like the United Kingdom have started developing and passing national security regulations that could allow a government to block an ISP.

But Freedom House's Shahbaz points out that this creep toward increasing internet censorship is more complicated in practice than just flipping a switch. He adds that widespread internet shutdowns don't always have a repressive regime's desired effect. For better or worse, an internet blackout limits the government's ability to conduct digital surveillance on citizens. And it can foster camaraderie among citizens that can turn into even more powerful protest movements.

"This is a very blunt attempt to control the information space in Iran by simply just denying individuals access to all information," Shahbaz says. "And it's not going to work. Information is going to continue to spread by other means. And, actually, sometimes shutting off the internet just drives people to the streets."

More Great WIRED Stories

- The strange life and mysterious death of a virtuoso coder
- How Facebook gets the First Amendment backward
- The enduring power of Asperger's, even as a non-diagnosis
- How to opt out of the sites that sell your personal data
- What Google's Fitbit buy means for the future of wearables
- 👁️ A safer way to protect your data; plus, check out the latest news on AI
- 🏃‍♀️ Want the best tools to get healthy? Check out our Gear team's picks for the best fitness trackers, running gear (including shoes and socks), and best headphones.

Lily Hay Newman is a staff writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University. Additionally... Read more

STAFF WRITER

FEATURED VIDEO

How to Make Your Browsing Data More Private than a Thousand Incognito Windows

TOPICS IRAN INTERNET CENSORSHIP

MORE FROM WIRED

VIDEO

How to Make Your Browsing Data More Private than a Thousand Incognito Windows

Thanks to an assist from Congress, your cable company has the legal right to sell your web-browsing data without your consent. This is how to protect your data from preying eyes.

WIRED

MORE FROM WIRED

CONTACT

RSS

Site Map

Accessibility Help

Condé Nast Store