VICE World News

How to Bypass ‘Digital Dictatorship’ During the Myanmar Coup

A guide to preparing for internet shutdowns, and how to communicate more safely when online.

MC By Michael Caster

February 7, 2021, 10:31pm Share Tweet Snap

PROTESTERS HOLD SIGNS DENOUNCING THE MILITARY DURING A DEMONSTRATION AGAINST THE COUP IN YANGON ON FEB. 8, 2021.
STR / AFP

Within the first week of the military seizing power in a coup on Feb. 1, Myanmar has already been plunged into two internet shutdowns: first, as soldiers arrested Aung San Suu Kyi and top leaders, and then several days later, as protests against the junta spread around the country. Between shutdowns, telecommunications providers restricted access to Facebook, WhatsApp, Twitter, Instagram and other platforms.

In trying to cut off a burgeoning civil disobedience campaign and hide abuses from the spotlight of social media or a globally connected population, the military has resorted to the blunt force of digital dictatorship. The target of the global #KeepItOn campaign, Internet shutdowns are on the rise around the world as authoritarians try to stymie resistance to their rule, but research from Ranking Digital Rights suggests they are often actually ineffective at quelling protest. Worryingly, instead shutdowns have been linked to greater risk of violence at demonstrations. The need for good communication security is all the more pressing for that reason.

In Myanmar, if the past week is an indication of things to come, the new normal may well be ongoing episodes of Internet disruption and digital insecurities.

For journalists, human rights defenders, and other members of civil society, these are challenging times, to say the least. But there also have never been so many new tools and tactics to fight back against repressive regimes. Although many of the tools designed for use during an Internet shutdown require the Internet to initially download and set up, knowing what's out there might help prepare for the next wave. Here's a step by step breakdown of some of the best options out there, how to use them, and where to find more resources.

World News

Myanmar Military Blocks Facebook As Dissent Over Coup Grows

HEATHER CHEN

02.03.21

How to Communicate During an Internet Shutdown

While you need the Internet to first download or setup, there are a few messaging apps that can be used even when data goes dark. One strategy on all of these applications is to first download them as Android Package Kit (.apk) files, and then they can be shared and installed on other devices without additional downloading. This is great for later sharing files with those who haven't managed to download them. For most of these apps you can often find the .apk file on the developers' website. For a more detailed breakdown, Brooklyn-based WITNESS has an excellent guide to communicating during Internet Shutdowns.

So-called Mesh Networks create peer-to-peer channels that allow for communication directly between devices even when the mobile data network is down. Instead of sending a signal from your phone to a cell tower to connect to the mobile network and then onward to the next device, mesh networks cut out the intermediary. They do this by allowing phones to communicate directly via their internal Bluetooth or WiFi antenna, but range can be woefully limited, around 100 meters (320 feet). Some apps do better, if multiple synced devices are within range then connectivity can travel along the chain for greater distance.

Mesh networks are good for communicating at a protest during an Internet shutdown or within a neighborhood, for example, but not so much internationally. Like all tools, they have limits.

Briar markets itself as "a messaging app designed for activists, journalists, and anyone else who needs a safe, easy and robust way to communicate." It creates end-to-end encrypted messaging, which means only the sending and receiving devices can read the messages, not the app company, telecommunications provider, authorities or other third parties. In addition to direct messaging, Briar supports private groups and public forums. You can also use Briar when there is Internet, but when connecting during a shutdown the range is limited to Bluetooth and WiFi. Briar is not available on iPhones.

News

How Internet Shutdowns Became a Weapon of Repression

MILENA MIKAEL-DEBASS

01.22.20

Bridgefy, another mesh networking app, gained considerable following in 2019 during protests in Hong Kong, making it a clever option as Myanmar joins the Milk Tea Alliance, an informal pan-Asian alliance fighting for democracy. Like Briar, Bridgefy functions during an Internet shutdown by creating a network between devices using the internal Bluetooth or WiFi antenna, but Bridgefy has some added features over Briar that make it the more popular choice.

Bridgefy can span greater distances. For example, with two devices about 100 meters apart your range is limited but if there's a third device another 100 meters now your range is effectively 200 meters. Add five Bridgefy users into a network with each device around 100 meters from the next and you've potentially created an encrypted network with a range four times larger. Basically, the more synced devices in a Bridgefy network, the farther you can communicate. With a security upgrade October last year, the app is even better than ever. Bridgefy is available for both Android and iOS (iPhone).

Until more people are using apps like Bridgefy to create expanding mesh networks, during a shutdown many will still be forced to rely on normal phone lines, assuming these haven't been cut too.

PROTESTERS HOLD SIGNS WITH THE IMAGE OF DETAINED CIVILIAN LEADER AUNG SAN SUU KYI AS THEY MARCH ALONG A STREET DURING A DEMONSTRATION AGAINST THE MILITARY COUP IN YANGON ON FEB. 8, 2021. PHOTO: STR / AFP

One of the security concerns of Internet shutdowns is precisely because they force you to communicate on the less secure GSM network (think 2G). While you may be able to make phone calls or send and receive text messages over the GSM network even during a shutdown, it is insecure and more vulnerable to surveillance. Luckily there are some ways to better protect yourself even when forced to rely on such insecure earlier generation networks.

Silence App has been getting attention as an open-source mobile phone application to encrypt SMS and MMS messages. As long as both sending and receiving parties have the app they can send encrypted text or multimedia messages. However, while the content of the message itself may be encrypted, third-parties may still be able to monitor who you are messaging with and when. It doesn't prevent your phone from being tracked either. There are also some questions about how well the application is being maintained by its developers and it isn't available on the Google Play Store.

Then there is Tella, an excellent option for secure documentation. It is an especially useful tool for journalists and human rights defenders since one of the rationales behind shutting down the Internet is to disrupt the documentation or reporting of abuses to the outside world. In addition to its customizable media collection features, Tella allows you to store any documentation data, photos or video for example, in an encrypted file on your device separate from the main gallery. This makes it much harder to find should your phone fall into the wrong hands, such as police officers during mass arrests. Some of its features do require later Internet connectivity, such as automatic upload to a secure server. WITNESS also has a great guide for documentation during shutdowns.

World News

Viral Woman Who Danced Through Myanmar Coup Tells Us What Happened

CAPE DIAMOND

02.02.21

What About When the Internet is Available?

Part of the reason blocking Facebook in Myanmar can be so detrimental is that tens of millions of people access online content almost exclusively through the platform, relying extensively on Facebook Messenger. This is a security nightmare. That's why those of us in the human rights and digital security communities around the world have been encouraging people to stop using Messenger and switch to more secure platforms: end-to-end encrypted messaging applications.

Signal is perhaps the industry standard end-to-end encrypted messenger. You can use Signal to chat directly between two people or create secure group chats, with up to 1,000 members. In December 2020, Signal also added a secure group calling feature which can include up to 8 people. Two-party secure calling had been available for some time. It is available for Android, iOS, and supports both a mobile and desktop version. The California-based Electronic Frontiers Foundation has an excellent guide on installing and setting up Signal for iOS and Android, among many other resources.

> **"Part of the reason blocking Facebook in Myanmar can be so detrimental is that tens of millions of people access online content almost exclusively through the platform, relying extensively on Facebook Messenger. This is a security nightmare."**

Another great end-to-end encrypted messaging app, Wire, uses the same encryption algorithm as Signal but has the added security feature which Signal doesn't have that you can set up your account without registering a phone number. This creates added anonymity. Also, Wire can handle secure video calling for up to 12 people and audio calls for as many as 25 people. Wire also works across all major mobile and desktop operating systems.

In Myanmar, the initial Internet shutdown following the coup targeted mobile data networks but left in-home broadband or fiber optic data connections somewhat intact. Admittedly, because most people in Myanmar rely on mobile devices for data access just targeting mobile networks was still highly disruptive. While we don't know how the military will behave moving forward, there is a good chance that disruptions may continue to target mobile networks first. This means, for those fortunate enough to have in-home broadband and computers, downloading Desktop applications is smart, in case you can't use them on your mobile device.

What About Accessing the Internet Itself Securely?

Many people may have heard of VPNs, Virtual Private Networks, but despite how easy they are to use people still seem intimidated by the idea of using a VPN to bypass online censorship or access the Internet more securely.

This is how a VPN works. If you are using a computer in Myanmar without a VPN, any website or server you access is likely to be able to see that your computer is in Myanmar, because your IP address will give this away. If there are websites that have been blocked inside the country, you also can't see them. If there are malicious online actors targeting journalists or human rights defenders based in Myanmar, you may be at risk. A VPN hides your true IP address and helps you get around blocks or insecurities such as these. Crucially, when connected to a VPN, your data is securely connected to a private server rather than the local Internet service provider (ISP). It masks your IP address and provides a high degree of anonymity.

There are a lot of VPNs on the market, some developed with journalists and human rights defenders specifically in mind. Some are free and others offer premium packages that range in price. The Electronic Frontiers Foundation has a detailed guide on selecting VPNs.

While there are plenty of choices, a few VPNs stand out for use in Myanmar right now. TunnelBear has a free version, but limits browsing to 500MB. That's about 6 hours of mostly text-based Internet browsing. The paid version allows for unlimited browsing. EngageMedia and others are already helping civil society with free access. Psiphon also has a free version with unlimited browsing but at very slow speeds. One added advantage of Psiphon is they already have a download page in Burmese, here.

Censorship

Here's Why Internet Shutdowns During Protests Should Worry Everyone

PALLAVI PUNDIR

12.18.19

Moving forward in Myanmar, understanding and adapting new tools and tactics for online communication and security is crucial. This is by far an incomplete overview, and good security needs a lot more than just apps, but hopefully it presents some insight for staying safe and staying in touch in the face of digital dictatorship.

Michael Caster is the Asia Digital Programme Manager at ARTICLE 19, a London-based organization supporting freedom of expression across the world. Follow him on Twitter here.

TAGGED: BURMA, WORLD POLITICS, WORLDNEWS, MYANMAR COUP, INTERNET SHUTDOWNS