Internet Shutdowns and Blockages

Dari دری
https://docs.google.com/document/d/1KZhHh38m0g1M6pb0cx5bveHqasTCXh_ueCnh2hs86kA/edit?usp=sharing

All of this only helps if you download these tools before censorship or network shutdowns happen. Your use of these tools can often be detected by your Internet provider, and show up as installed apps visible to anyone looking at your unlocked phone.

Dedicated anti-censorship tools:

- **Psiphon** is a free and open source censorship circumvention VPN that uses a variety of techniques to bypass Internet censorship
    - https://www.psiphon3.com/en/download.html (iOS, Android, Windows)
    - *Download via email:* Send an email to *get@psiphon3.com* to receive mirror download links of Psiphon in multiple languages.
- **Lantern** is a free and open source censorship circumvention VPN that uses a variety of techniques to bypass Internet censorship.
    - https://getlantern.org/en_US/index.html (Windows, MacOSX, Linux, iOS, Android)
- **Tor Browser** is the de-facto anonymity web browser that uses the Tor network for improved anonymity and provides censorship circumvention.
    - https://www.torproject.org/download/ (Windows, MacOSX, Linux, Android);
    - *Download via email:* Send a request to GetTor (gettor@torproject.org) specifying your operating system (and your locale). Ex: "windows fa"
    - **OnionBrowser** (iOS) https://onionbrowser.com https://apps.apple.com/us/app/onion-browser/id519296448

VPNs with good anti-censorship track records:

- **TunnelBear** - https://www.tunnelbear.com/download - (Windows, MacOSX, Linux, iOS, Android)
    - **NOTE: Tunnelbear is currently free for users in Afghanistan for up to 10G/month. Not available in Google App store, but users can download an APK from the official Telegram channel (Global) https://t.me/tunnelbearofficial**
    - If people are having problems connecting to Tunnelbear, report issues: https://forms.office.com/Pages/ResponsePage.aspx?id=jONDSdRtjEKIbSSTK8LV3qF7yXc9pWZBuoBU9l0NfhJUREEyUlBTUFZSNzRONFY3R0kwWFBTTVRWTS4u&locale=fa
- **Mullvad** - https://mullvad.net/en/download/ (Windows, MacOSX, Linux, iOS, Android) €5/month ; free licenses available from helplines like help@accessnow.org
- **Bitmask** - https://bitmask.net/ (Windows, MacOSX, Linux, Android) is an open source VPN. You can use a built in provider or start your own.
- **VPNGate** - https://www.vpngate.net/ (Windows, MacOSX, Linux, iOS, Android) a list

of public VPN relay servers hosted by volunteers around the world.
- **ProtonVPN** - https://protonvpn.com/ (Windows, MacOSX, Linux, iOS, Android, Chromebook) Free tier available.

Many other VPNs are out there, but not all have made efforts to evade censorship or have good and proven security, privacy, and business practices. This review is a good place to start if you are looking for additional options: https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

A good resource for how VPNs work, what they do and what they don't help with is here: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you. Please note that most (if not all) VPN "review" sites profit off of VPN purchases and/or are owned by the same companies which own the VPNs.

Total Shutdowns

Consider preparing for a complete shutdown, whether caused intentionally, or by a power outage or natural disaster, and making basic plans for what tools to try and use with friends/colleagues and/or where to gather if safe. These tools all have security concerns, hardware costs, legal barriers, and require some level of "density" of technical users to work.

Note: Any "mesh" style app is going to be a trade-off in terms of privacy/anonymity and possibly security as well. For apps to "participate" in a peer to peer mesh, they must broadcast their intention to join, which can be surveilled and tracked, even if the messages sent are encrypted.

- **Briar** https://briarproject.org/download-briar/ (Android) Briar will use Tor if available, or wait and connect with other Briar users over bluetooth or wifi when in range so send messages. Only works if people are close enough for bluetooth (30m) or wifi (100m max)
- **Bridgefy** https://bridgefy.me/demo-app/ (iOS/Android) - Bridgefy is less secure, but has been working to improve their message security; but they have yet to establish a track record on security or trust with the broader security community. It works across platform, which is useful.
- **Silence.im** https://silence.im/ (Android) Provides encrypted chat over SMS, so if SMS is still working and both parties have the Silence app, you can communicate securely.

Also useful
- **F-Droid** https://f-droid.org (Android) (trusted Android app sharing, if both phone have F-Droid, they can swap apps even without Internet: https://f-droid.org/en/tutorials/swap/)