The Cloak

Emerging Tech Use Case

Cyber security • IoT • Blockchain

Table of Contents

The author **Asad Ayub** is a World Economic Forum Global Shaper. He believes in harnessing emerging technology for the greater good.

The Context

This handbook details how to use a specific combination of emerging technologies. This combination is called, *The Cloak*. Using *The Cloak* is not a measure of first resort and is usually deployed under extreme circumstances. To illustrate what this means, I present a possible fictional scenario below where *The Cloak* might be deployed.

You are working at the head quarters of a large non-profit called *Educat-her International* in a developed country. Your organisation has built schools in a developing country called Menya, where they feed two meals a day to five million girls with the help of your local sister non-profit organisation *Mamboo*.

A violent military coup in *Menya* results in a military junta to be installed. The military junta is cracking down on non-profits drawing international funding on the suspicion of spying for foreign powers. *Maboo*'s bank accounts are frozen and without the funding from your organisation the children are at risk of going hungry due to extreme poverty.

This handbook illustrates how *Mamboo* can use *The Cloak* of Invisibility to continue to receive some (if not all) the funding from *Educat-her International* so that you can make sure the little girls don't starve. To do that we must educate you in a bit of blockchain technology, a bit of cyber security and a bit of IoT.

Who needs it

This handbook will be of use to those fighting for social and environmental justice in a country where the state is hostile to such activities.

01

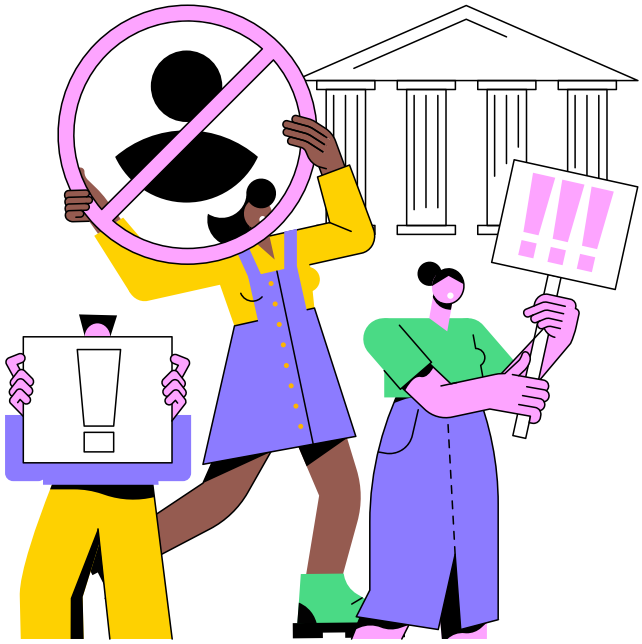
Human Rights Defenders

10

Persecuted Minorities

02

Human Rights Lawyers & Activists



08

Environmental Activists

03

Labor Unions

07

Journalists

04

Whistle Blowers

06

Indigenous Defenders

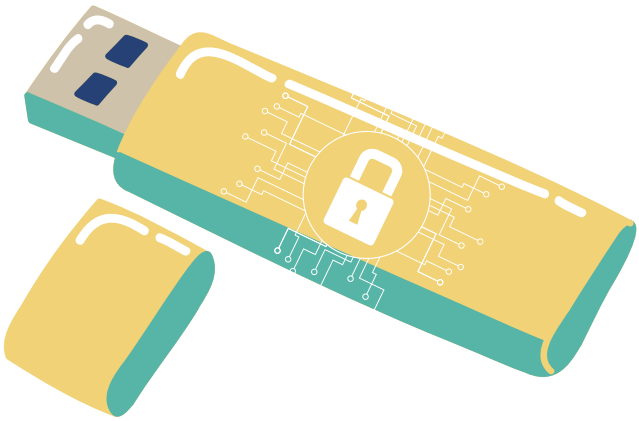
05

Social Activists & Protesters

Cyber Security

The team from *Mamboo* must now learn to communicate with you while being invisible online.

Being Invisible



In countries such as our fictional country of *Menya*, people who are deemed a threat to the status quo are easy to surveil thanks to the GPS in smart phones.

Usually when the police raids the houses and properties of the suspected climate/social activists and gets access to the passwords of the laptops and cell phones from the owners of the devices with the threat or use of violence.

The cyber security part of *The Cloak* makes sure that there are no digital traces of your communications when the evil junta breaks into your apartment and confiscates your laptop. For that *Mamboo* needs *The Cloak* of Invisibility.

There is no way to secure a smartphone so I would not suggest using a cell phone or a smart phone at all if you are a social or environmental activist in *Menya*.

Tor Network

The Tor Network is what you use to access the dark web.

What 01

The Tor network is a decentralised, open source, volunteer-operated network designed to provide privacy and anonymity to users on the internet.

02 How

It achieves this by routing internet traffic through a series of encrypted nodes, or relays, in a way that obscures the user's identity and location.

03 Who

Journalists, activists, and whistleblowers also rely on Tor to communicate and share information in a secure and anonymous manner e.g. places like *Menya*.

Tails

VPNs are not enough if you want to be truly invisible you would need to use Tails. Tails is a portable operating system that protects against surveillance and censorship using the Tor network.

01 Download

Download Tails software from Tails.net

02 Copy to USB

Get a usb with minimum 8GBs. Install Tails to the usb.

03 Plug & Play

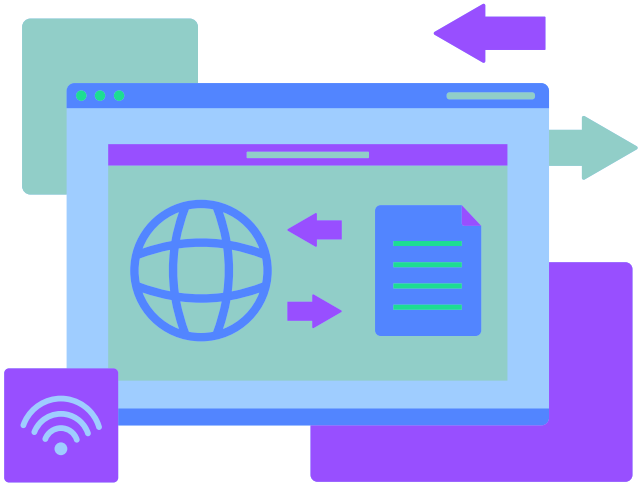
The next time you plug in the USB you can now have a more secure operating system within your original operating system - that is Tails. Every time you unplug, all the data gets erased.

Tails

Features and Functions

01 No Trace

Unlike a regular operating system, the memory is entirely deleted when you shutdown Tails, erasing all possible traces. It doesn't use your PC's memory.



02 Useful Apps

Tails includes:

- Tor Browser with uBlock, a secure browser and an ad-blocker
- Thunderbird, for encrypted emails
- KeePassXC, to create and store strong passwords
- OnionShare, to share files over Tor
- Electrum bitcoin wallet

03 Tor

Everything you do on the Internet from Tails goes through the Tor network. Tor encrypts and anonymises your connection.

Whonix-Qubes

Features and Functions

01 What

Whonix-Qubes is also a virtual machine within your computer like Tails, except it is for longer term use. Tails is plug and play so you will have to re-install everything from scratch every time.

02 How

Download and follow the instruction on: whonix.org/

03 Privacy coins

Monero CLI/daemon + Qubes + Whonix

You will understand this point better after reading the chapter on blockchain technology. I just want to note that with Whonix-Qubes you can have enhanced privacy for transactions with your Monero wallet.

Blockchain Technology

The team from *Mamboo* has made contact with you and they are invisible - now they need money to keep the children fed. Let us see what we can do with the help of decentralised finance.

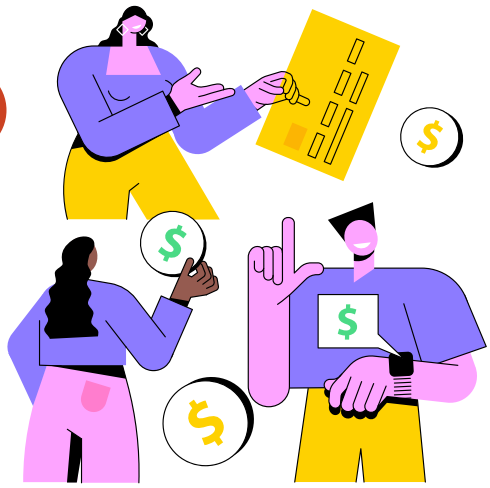
Privacy Coins

Although blockchain is an entirely open & transparent decentralised ledger - there are ways to become invisible. One of these ways is by using privacy coins such as *Monero*.

Privacy Coins

01 Make a wallet

Get a Monero wallet for Whonix-Qubes. This is the option we will explore on this page. There are other ways such as using an Electrum wallet for Tails (Bitcoin Lightening Network).



02 Secure your keys

You have to make sure that you find a clever way to write down and secure a few copies of the keys or pass phrases for your wallet. Without this, all the money in your wallet will be lost!

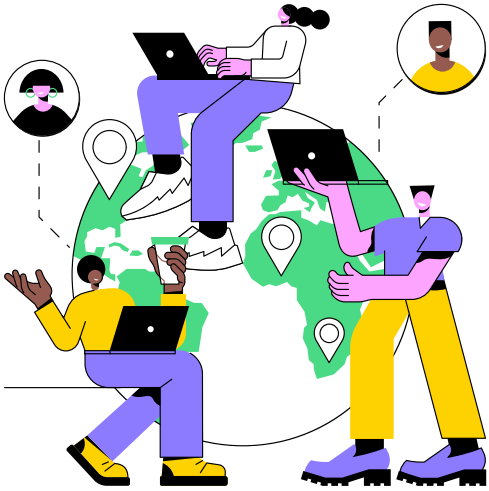
03 Cold Storage

The best way to store your coins is by storing your coins offline - in a cold wallet i.e. a hardware wallet such as Trezor or Ledger. There is also such a thing as paper wallets for physical transfer of coins.

Privacy Coins

Convert 01

First you will have to convert your local currency into a privacy coin using one of the crypto exchanges which do not have strict KYC (Know Your Customer) policies.



02 Send

Then you will have to make sure you are invisible and send the wallet keys or the privacy coins them selves to the wallet of your choosing. If you misspell the wallet address then your coins are lost for ever so be careful.

03 Recieve

Mamboo from our example will be receiving the coins and will have to get them converted using a decentralised exchange or through informal markets such as those close to border towns.

Mixers & Tumblers

Mixers and tumblers enhance the privacy and anonymity of cryptocurrency transactions by mixing or tumbling different users' coins together before sending them to their intended destination which makes it harder to trace.

Mixers & Tumblers

Deposit 01

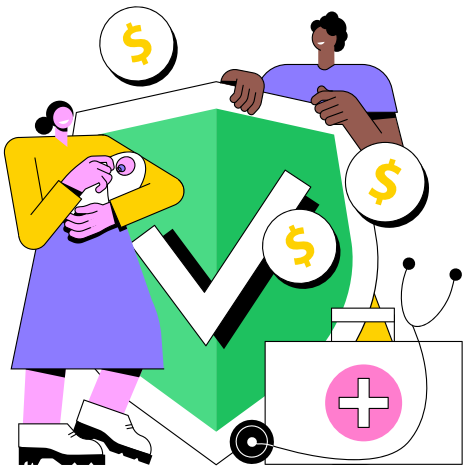
Users send their cryptocurrency to a mixing or tumbling service, usually through a designated address provided by the service.

02 Mix

The mixing or tumbling service collects and combines funds from multiple users into a single pool. This mixing process aims to break the direct link between the sender and recipient addresses.

03 Recieve

The mixer or tumbler service sends the equivalent amount of cryptocurrency back to the users' specified addresses. These output transactions make it challenging to trace the original source of the coins, as they now appear to come from various sources.



IoT

There is a way that combines cyber security, Internet of Things (IoT) and blockchain technology.

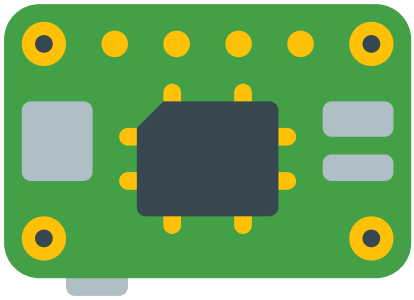
Bitcoin Lightening Network

The Bitcoin Lightening Network allows for invisible transactions by using a layer on top of the regular Bitcoin blockchain that allows you to send and receive small payments quickly and privately. Both parties must run a lightening network node. This involves a bit IoT (Internet of Things) magic using a tiny computer called Raspberry Pi.

Lightening Node

Purchase & set-up a Raspberry Pi 01

You will need a Raspberry pi 4, a 1 terabyte solid-state drive (SSD), an SSD enclosure, a 16 gigabyte or larger microSD, an ethernet cable and a power source. Install a compatible operating system.



Download Bitcoin Lightening Network 02

Set-up a Bitcoin Core node and then install a Lightening Network software for Raspberry Pi such as LND (Lightning Network Daemon), Umbrel node, myNode and RaspiBlitz etc. You will need a few days to set this up and download the Bitcoin ledger.

Send & Receive 03

Set up your Lightning node's configuration, including creating a wallet, setting up a Lightening Channel, and generating a Lightning Payment Request. Now you can send and receive Bitcoin on your Lightning Node.

Flipper Zero

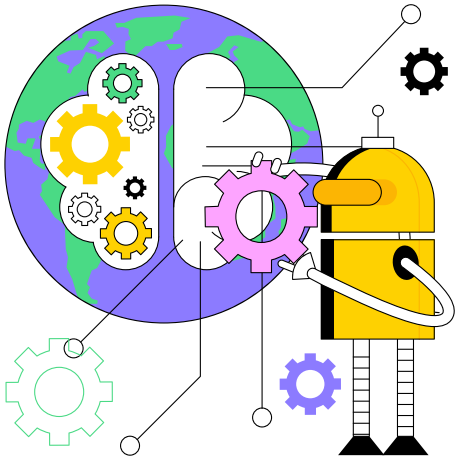
Most of the surveillance and security devices that are being used to track people by authoritarian regimes are built using outdated legacy software and technologies that are very easy to hack if you have the right tools or knowledge. Flipper Zero is one of those tools. Flipper Zero is a multifunctional open-source hardware device which can help individuals avoid certain forms of surveillance.

Flipper Zero

Purchase or build this device

01

Since it is open-source hardware, it should not be hard to put it together yourself or with the help of an engineering or IT university student using a Raspberry Pi.



Signal Analysis and Jamming

02

Flipper Zero can help you understand wireless signals like Bluetooth or RFID. If you think someone's trying to connect to your devices without permission, Flipper Zero might help you spot and stop them. It's like having a radar for unwanted connections.

Disabling or Modifying Devices

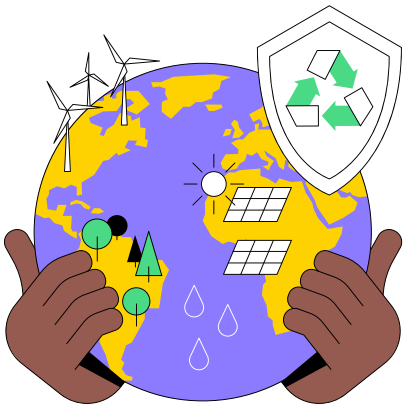
03

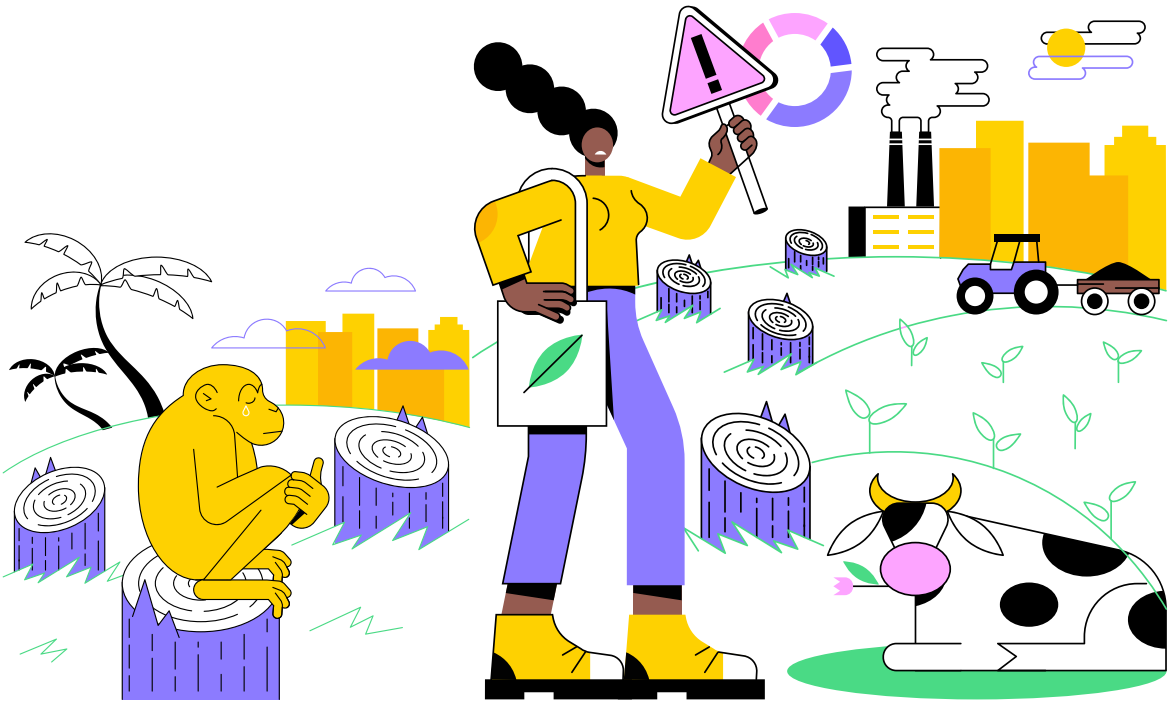
Sometimes devices collect data without us knowing. With Flipper Zero, you might be able to change or stop these devices from working temporarily. But be careful and follow rules – it's like using a tool to put something on pause for a bit.

Voila!

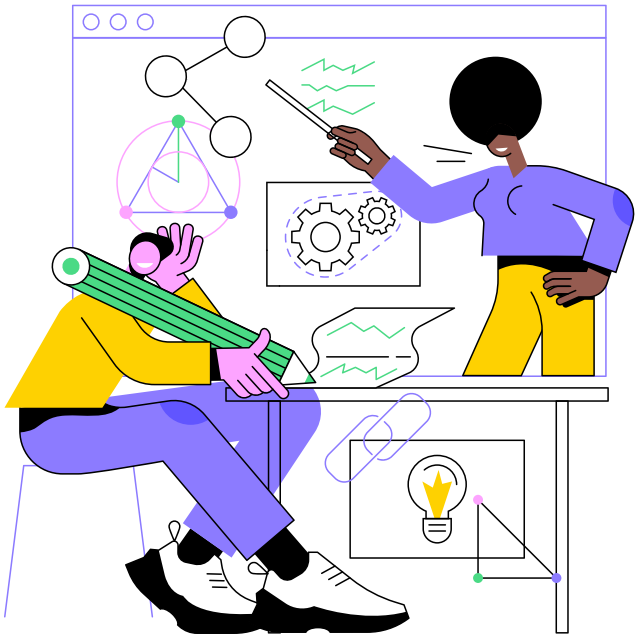
The team from *Mamboo* is now invisible and you are in contact with them. They can now receive money from *Educate-her International*. 5 million school girls in *Menya* are having two meals a day thanks to you and your teams ability to leverage a variety of emerging technologies called *The Cloak*.

Thousands of environmental defenders have died in the past decade.

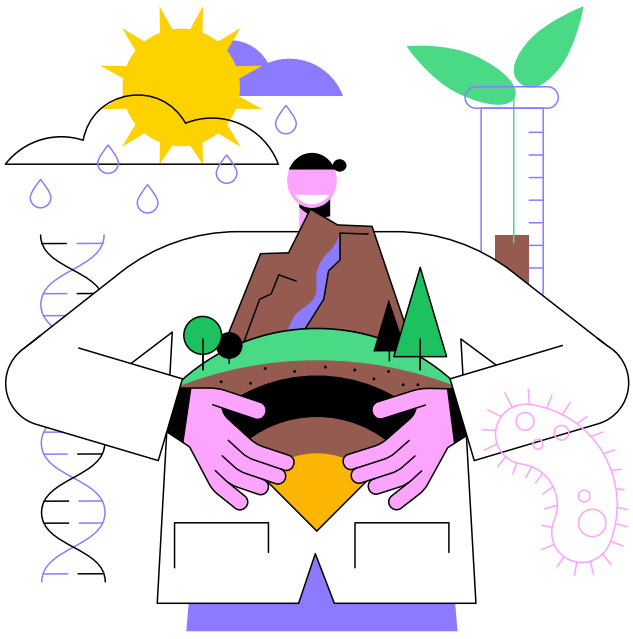


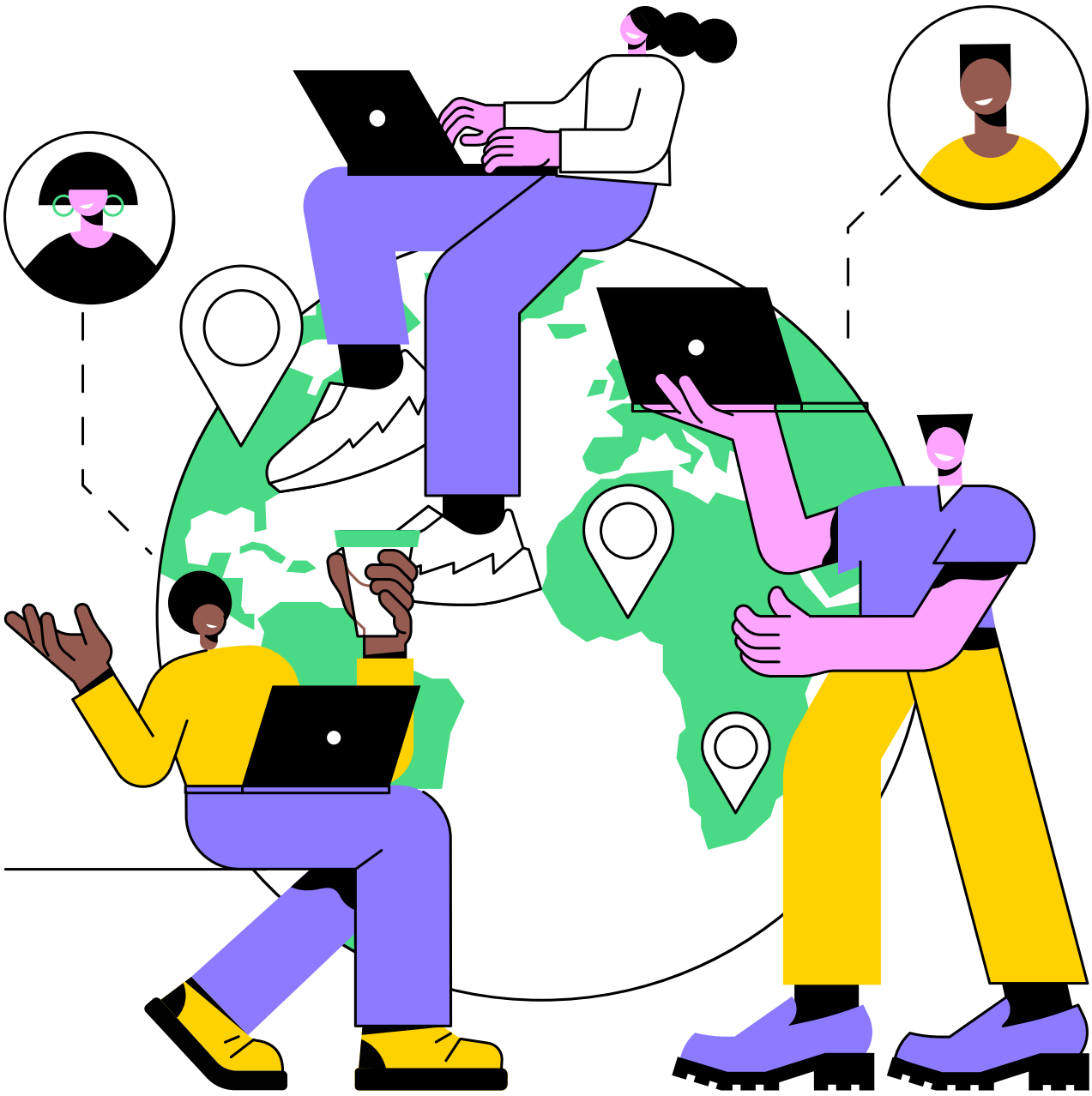


Indigenous rights defenders accounted for almost a quarter of all human rights related killings.



Tools like The Cloak might help save a few.





About The Author

Asad Ayub is an award winning social entrepreneur. He has worked on projects for the EU, MasterCard Foundation and Google.org.