

Challenges, needs and opportunities for digital rights organizations in the Global South

Between March and April of 2022, we interviewed contributors of digital rights organizations from multiple countries to understand the challenges they have faced in the past year, their needs for improving their digital security and to strengthen their work.

Countries

Colombia, Guatemala, Kenya and Tanzania

Colombia

The past year was really challenging for our partners in Colombia. With the National Strike (*"Paro Nacional"*) the country experienced what was called by many as a "war climate". Activists disappeared, suffered kidnapping, incarceration and even assassination. In the digital rights field, activists tried to support grassroots movements to take care of their data and secure their activism. There were reports of internet shutdowns in some cities during the protests, as well as internet filtering on specific websites that were reporting about the National Strike.

Our partners experienced higher demand for continued (rather than one-off) training with high risk activists and those who suddenly became a public personality because of the protests.

Our local partners also highlighted that *campesinos* and indigenous populations are becoming more concerned about digital security, and mentioned the need for collaborative training methods and

localized materials about digital rights with those communities.

Opportunities

- Continue training local communities
- Increase awareness among *campesinos* and indigenous populations
- Monitor, detect, and plan actions against censorship events during protests

Risks

- Open Source Intelligence collection and social media monitoring by adversaries
- Kidnap, incarceration, and assassination of social leaders and activists
- Online harassment

Needs

- Localized digital security materials for different communities (*campesinos*, indigenous)
- Digital security training for these other communities
- Digital rights literacy materials
- In person trainings
- Funding for participants of the training sessions

Quote

"It helps a lot that people can get to know who develops the tools. That is why it is always very good when you come, it creates an invaluable confidence. That's why I think visits make a lot of sense. And in general, we need to build more alternatives and develop more skills on the internet. A holistic work between the digital, because we are advocating for a field that is not a priority because there are many threats that people identify as more serious. (...)"

I think it's very easy to get overconfident with the tools 'if I use signal/tor/etc I'm free from any digital threat' and that's not true. (the holistic work) to think as a set of practices."

Guatemala

As with many other countries, our partners in Guatemala are experiencing fatigue with online tools. However that hasn't stopped their work, as the threats faced have increased in the past year. They reported that the website of the organization [Fundación Acceso](#) was blocked for over a year (in 2020 and 2021), with no explanation.

They received recurring requests for digital security training and continued follow up, and developed a 90 minute training method to reduce fatigue and engage participants. During this period they also audited many systems looking specially for the NSO Group's Pegasus technology.

Using open source tools can be challenging for some participants, so they have also worked to support users shift from big companies like Google to other tools.

They are developing a system to support onion sites, Tor Browser, Nextcloud and other tools on simple hardware like the Raspberry Pi, to support activists and journalists.

Opportunities

- Continue digital security training
- Increase awareness among indigenous communities in the region
- Advocate Tor Browser for Android for young indigenous media activists

Risks

- Incarceration of activists
- Unexpected censorship of NGO websites

- Threats against *campesinos* and indigenous communities
- Harassment against feminist movements
- Pegasus spyware infection

Needs

- Raise awareness about how, when and why to use Tor in practice
- Contact with the Open Observatory of Network Interference (OONI) to partner on monitoring specific censorship events

Quote

"I think that perhaps one of my perceptions is the need to understand what are the use cases of Tor. So, eh... and if you want to use it all the time. If you want to make all your internet connection torified, what does it imply? Is that what you need? Or what you want is to be anonymous, do anonymous searches, maybe you don't have to enter Google using Tor, or what does it mean to be constantly browsing the internet with Tor, and captcha appears? (...) I think that the use case is something important to understand, and then what you win and what you lose when using Tor."

Kenya

As Kenya prepares for general elections in 2022, digital rights activists are still struggling to find good internet bandwidth.

When the pandemic hit and everything became remote, digital security training followed the same path, which was a challenging due to the cost and speed of internet data bundles.

During meetings with journalists, activists and others, our partners have experienced zoom bombing as a way to disrupt their activities and intimidate them.

In the digital rights field, they are also looking for VPNs to protect their connection and communication. Some

organizations have also requested audits of their digital systems and websites.

Opportunities

- Continue Tor training
- Make recommendations for digital security tools
- Fund more digital security training
- Fund research into Tor uses in the region

Risks

- Misinformation because of the elections
- Zoom bombing

Needs

"I want to do research on how Tor has been received in Kenya, because it is becoming a popular tool here."

Quotes

"We say that the internet slowdown is the new internet shutdown."

"People can't stand any more meetings online"

Tanzania

Our partners in Tanzania raised a lot of concerns about physical security, as well as their need to increase digital rights not only with their communities, but within their own organization too. Similar to Kenya, internet bandwidth is not sufficient to run online trainings with many people from their communities, so the training they performed in the last year was in person. Instead, they were required to travel to the communities, buy expensive internet data bundles and provide some financial support to the participants too, in addition to other administrative costs, raising the total cost of the training significantly.

Opportunities

- Increase digital security with LGBTQ+ communities in the region
- Strengthen digital security knowledge within the organization
- Localize material in Swahili

Risks

- Robbery in their headquarters
- Eviction due to prejudice against LGBTQ+ communities

Needs

- Funding for more digital security trainings with LGBTQ+ communities in other cities
- Increase their headquarter security (needs for funders)
- Translation of the material to Swahili as many of their community don't speak English
- Digital security trainings for their organization

Quote

"Make sure to support the shift security in the organization so we can support the community. It's very hard to clean other people's houses when your house is not very clean. So if you can help the organization first, so it's more tangible and successful, we can go to the community."

Conclusion

Most partners expressed their need for funding to support digital security training with their communities, as well as to raise awareness of Tor as part of a holistic digital security practice.

They also mentioned their work has increased with *campesinos* and indigenous communities, including training for Tor Browser for Android.

The translation and localization of continually updated materials is a key point mentioned by most partners.