

Undertaking the crucial task of bringing cryptography to activists

Wednesday 20 February 2019, by [CASSAUWERS Tom](#) (Date first published: 11 February 2019).

A group of journalists and activists slowly trickle into a room. They take a seat. Some talk amongst each other, others play around with their phones. They think they are there for a workshop, but unbeknownst to them, they are being hacked. Five minutes after their arrival, a security expert has cracked most of their phones, and with it, sensitive information about contacts, co-activists, planned protests and stories.

The story is real, yet nobody got hurt. The course was organised by the Dutch NGO Free Press Unlimited and the hacking is part of a workshop where they try to show journalists and activists the importance of online security. Shock therapy, if you will.

But in real life this sort of incident is not exceptional. Authoritarianism is on the rise globally, and with it, the repression of activists and journalists. And this doesn't just take place face-to-face, but also online. The computers and phones of activists are free game all across the world, particularly the Global South. Nevertheless, a new generation of cryptographic activists are bringing their specialised skills to the aid of other activists.

"Cryptography is very important for activists," says Jaap-Henk Hoepman, an associate professor at Radboud University in Nijmegen, the Netherlands, where he works on issues such as cryptography, privacy and online security.

"When activists do things that go against societal norms, particularly in less-democratic countries, they should exchange information and contacts in a secure way to prevent reprisals. And cryptography can help accomplish that."

Particularly because the amount of activists that live in at-risk countries is increasing. Freedom House, a Washington DC-based organisation dedicated to protecting freedom of expression globally, calculated that in 2017, 71 countries suffered a decline in civil and political liberties, while only 35 registered gains.

One of the activists who witnessed this rise of authoritarianism first hand is Sofia Celi. The cryptographic activist was originally based in Brazil, but moved back to Quito in Ecuador after the election of the extreme-right president Jair Bolsonaro in 2018, who repeatedly showed his admiration for the country's past military dictatorship. "We are close to activists in Brazil, but after the turmoil of the last months we decided to move back to Quito," Celi says.

Digital autonomy

Back in Quito Celi is working with the Centro de Autonomía Digital (CAD), a group of activists who work on cryptography and digital security. Their target group is fellow NGOs and activists in the Global South.

Usability is one of their key challenges. "Some projects took big steps in making their software usable, like the Tor Project," says Celi, referring to an open-source browser and network that allows users to browse the internet anonymously, and access websites that are not listed on the regular web. "Security experts often assume these things are easy to configure, but mostly they are not accessible to regular people. These tools are often based on beautiful mathematical proofs and concepts, but people often don't use them because they come with a high learning curve."

And this is of particular importance in the Global South. "Activists in the Global South are often much more vulnerable, and their governments much more repressive," says Celi.

"But the security community doesn't necessarily design for them, because they often assume activists in the Global South have access to high-tech software or even smartphones. This is not always the case. Some activists in the Global South, for example, have one computer which they share amongst 10 people."

Which is why CAD is designing a range of systems that are appropriate for all kinds of activists, wherever they are based. CAD is, for example, designing an anti-phishing system that recognises whether a received email is real or not. Phishing is a technique where malicious actors pretend to be someone else, and tries to steal sensitive information (like passwords).

And although more challenging mathematical-cryptographic research is attractive to Celi, she sees countering these types of lower-tech attacks as potentially much more impactful. "Of course it's more exciting to study deeply academic problems," she says. "But phishing is one of the most common security risks for activists, and building a defence against it is key."

Illegal cryptography

But how do cryptographers deal with unintended uses of their tools? Criminals, for example, use software like Tor just as activists do. A 2016 study from King's College London claimed that 57 per cent of sites on the Tor network contained illicit content.

"We need to be aware of the negative consequences of these technologies," says Hoepman. "But it's not the task of cryptographers to decide who can and cannot use cryptography. What we can do is communicate about its advantages and disadvantages."

For Celi usability again takes centre stage in dealing with this ethical problem. "We have a moral responsibility," she says. "Criminals will always find tools to do their business. That's why we need to make these types of technologies as accessible as possible, so that normal people and activists can use them."

Globally, journalists are another key group profiting from strong cryptography, and Free Press Unlimited supports journalists when they enter the area.

One field they specialise in is the rights of whistleblowers. "Today whistleblowers are often exposed after they leak information," says Leon Willems, director of Free Press Unlimited. "Most of the time they end up being worse off than before they leaked [the information]. Maybe they have to run away, maybe they suffer retaliation or maybe they lose their jobs. These people performed a public service, yet most of the time they are punished for it."

Which is why they developed a system, Publeaks, which is based on similar software called GlobaLeaks, to make whistleblowing secure and cryptographically protected. "We first tested the system in the Netherlands," says Willems. "Because if a mistake happens in this country, our relatively strong legal protections won't make people pay the ultimate price. And based on that

experience we are now supporting operations in Mexico, Nigeria and Indonesia.”

In Indonesia, a derivative of GlobaLeaks, called IndonesiaLeaks has already contributed to exposing a major corruption scandal with the support of Free Press Unlimited. Yet Free Press Unlimited is keen on emphasising the ownership that actors in the Global South exert over the technology. “It was their decision to use the software, which is called GlobaLeaks, and they own the project,” says Willems. “But we provided technical support in implementing the system.”

Irrespective of whether activists and journalists are based in Indonesia, Brazil or the Netherlands cryptography is becoming an increasingly important tool. And by hiding their own moves, rights defenders just might be able to expose those of the people whose wrongdoings need to be brought to the public’s attention.

Tom Cassauwers

[Click here](#) to subscribe to our weekly newsletters in English and or French. You will receive one email every Monday containing links to all articles published in the last 7 days.

P.S.

Equal Times

<https://www.equaltimes.org/undertaking-the-crucial-task-of#.XGzhMVRKjIU>