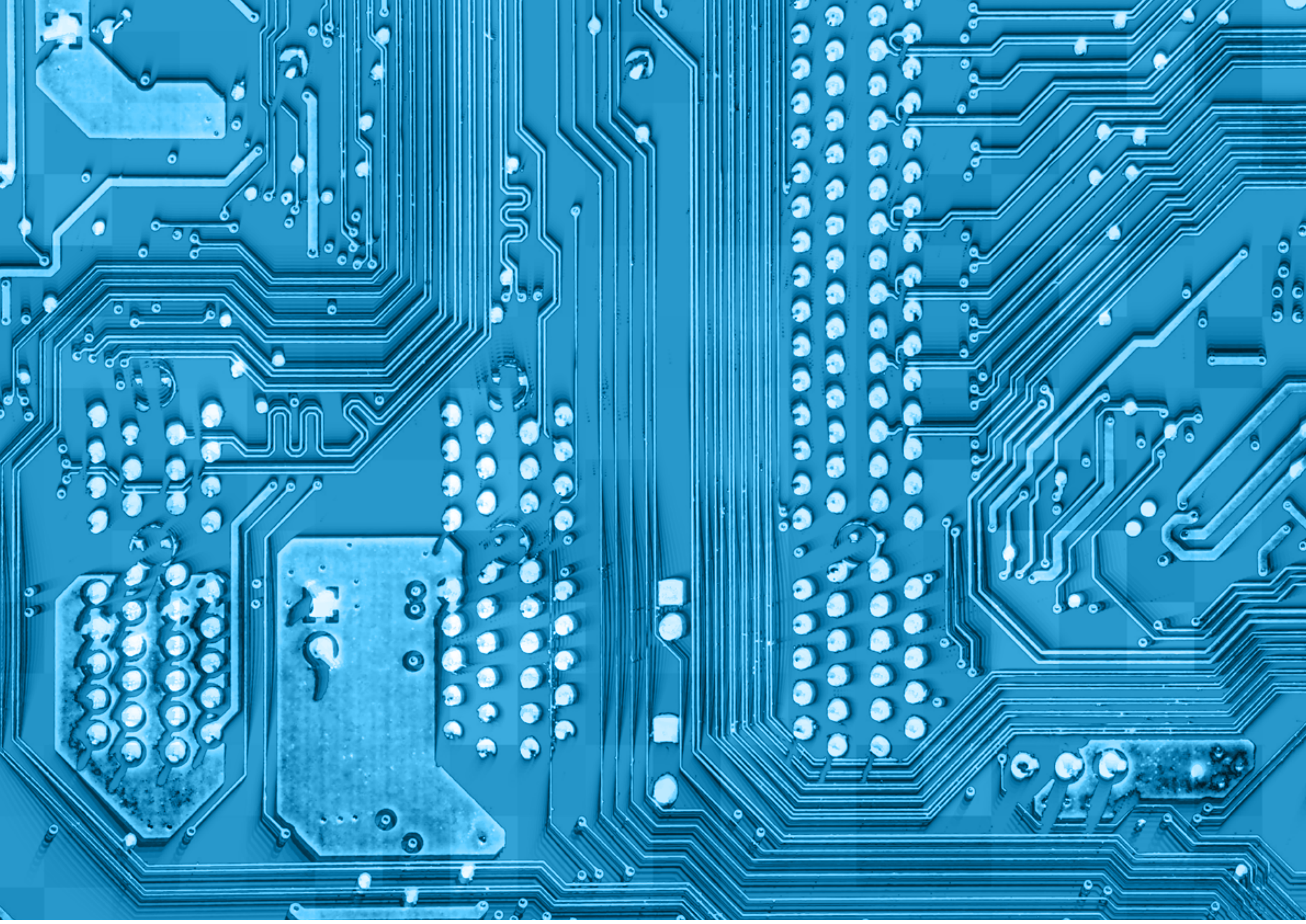
OPEN TECHNOLOGY FUND

# 2019/2020 ANNUAL REPORT

# Table of Contents

Layout design by **Ura Design**



01

# About This Report

This report covers the activities supported by Open Technology Fund (OTF), with a small number of exceptions for highly sensitive projects, from October 2019 to March 2022 with FY2019* and FY2020 funds.

*In April 2020, Radio Free Asia (RFA) assigned $6,844,550 in FY19 contracts to OTF Inc. This report includes details about those contracts along with all FY2020 contracts funded directly by OTF Inc.

# 02 A Message to Our Community

The world has changed in unimaginable ways over the past two years. As repressive governments around the world have deployed more sophisticated and aggressive measures to censor free speech and restrict access online than ever before, the internet freedom community has also been forced to contend with the many challenges of the global COVID-19 pandemic. Despite new challenges from COVID-19 and authoritarians alike, the internet freedom community has stood together to help those in Hong Kong, Belarus, Myanmar, Ukraine, Russia and elsewhere to fight for their rights and freedoms. In the face of incredible challenges, this community has continued to show its creativity, heart, and unwavering resolve to protect human rights online for everyone.

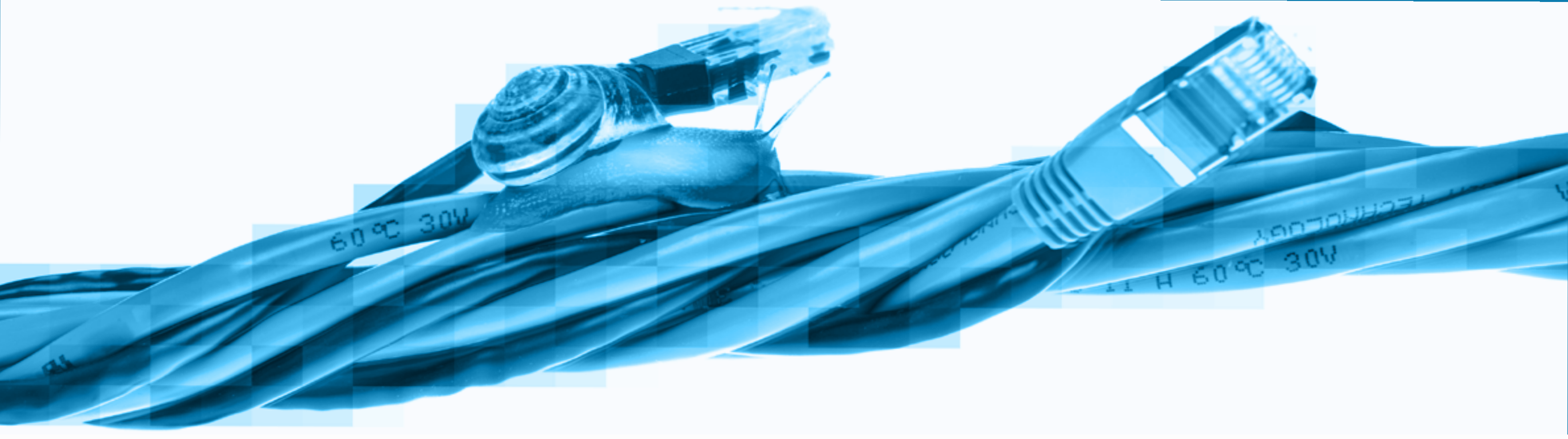
In addition to the many external threats faced over the past two years, OTF's very existence was also threatened. In June 2020, a new Chief Executive Officer, Michael Pack, was appointed to lead the US. Agency for Global Media, OTF's donor organization. Upon his confirmation, Pack immediately fired the leadership and dismissed the Board of Directors of all USAGM grantee organizations, including OTF. Pack then attempted to install new leadership at OTF and directed that all OTF's funds be frozen. Despite significant bipartisan condemnation from Congress, USAGM, under Pack's leadership, continued to withhold $19,181,790 in congressionally appropriated funding from OTF for eight months. As a result, OTF was forced to issue stop-work orders to 49 of its 60 internet freedom projects (80 percent of all programs) in July 2020.

In response to Pack's actions to remove and replace OTF's leadership and Board of Directors, the D.C. Circuit Court of Appeals quickly granted OTF a temporary injunction enjoining Pack from "taking any action to remove or replace any officer or directors of the Open Technology Fund." In addition, despite the funding freeze imposed, OTF continued to work to deliver on its important mission by collaborating with other like-minded donors to find external support for many critical internet freedom projects impacted by the funding freeze.

Thanks to the extraordinary outpouring of support from our community, our fellow donors, and our supporters around the world, OTF was able to fully resume normal operations in 2021. We are deeply grateful for and humbled by the support and solidarity that OTF received during this difficult and uncertain period, but more than anything we are thankful that we've been able to resume the truly important work of supporting critical internet freedom efforts globally. We would like to use this opportunity to thank all the organizations and individuals who stood up for OTF when the organization's future was in deep peril. OTF would no longer exist absent your tireless efforts and unwavering resolve. This annual report catalogs the projects that OTF funded over the past two years, but more importantly it captures the incredible efforts and accomplishments of our community and partners all around the world.

With the ongoing support of our community and partners, we are confident that OTF is stronger and more resilient than ever, and we're looking forward to all we'll be able to accomplish in the coming years together.

***The OTF Team***



# 03

# About OTF

The Open Technology Fund (OTF) is a Congressionally-authorized, independent non-profit organization dedicated to advancing internet freedom globally. OTF works to advance internet freedom in repressive environments by supporting the applied research, development, implementation, and maintenance of technologies that provide secure and uncensored access to enable citizens worldwide to exercise their fundamental human rights online. OTF is authorized by the U.S. Congress to "advance unrestricted access to the Internet in repressive environments" and is funded by the U.S. Agency for Global Media.

## Our Mission

OTF works to advance internet freedom in repressive environments by supporting the research, development, implementation, and maintenance of technologies that provide secure and uncensored access to the internet to counter attempts by authoritarian governments to restrict freedom online and enable all citizens to exercise their fundamental human rights online.

OTF supports projects in an effort to:

- **Provide unrestricted access to the internet to individuals living in information restrictive countries** to help ensure they are able to safely access the internet. This includes supporting the development and deployment of an array of circumvention technologies to counter increasingly sophisticated censorship techniques, new solutions to counter internet shutdowns, and applied research to help tool developers and users stay ahead of new censorship threats.

- **Protect journalists, human rights defenders, and marginalized communities from repressive surveillance and digital attacks** to help ensure they are able to safely access and share information online. This includes support for secure communication tools, targeted digital security interventions, and other forms of privacy and security technology.

# Our Approach

OTF provides funding and support through a variety of mechanisms in order to provide tailored and comprehensive assistance to internet freedom projects. Because internet censorship technology and tactics are constantly evolving, OTF receives, reviews, and contracts projects on an ongoing basis via open calls. OTF solicits project ideas through a fully open and competitive application process on its website. The process is designed to reduce barriers to applying for funding and make funding more accessible to qualified individuals and organizations around the world. These efforts help attract innovative applications from groups that traditionally are not able to apply for federal funds, including expert technologists, frontline journalists, human rights defenders, cutting-edge researchers, and digital security specialists.

In order to ensure a high degree of due diligence, OTF implements a rigorous multi-stage application review process throughout which successful applications are ultimately improved and refined. All proposals are reviewed by OTF's specialized staff of subject matter experts as well as OTF's Advisory Council—a group of nearly 40 technical, regional, and specialized experts from a wide range of relevant disciplines—to provide feedback and guidance. In addition to ensuring that the most competitive and impactful projects are funded, this multistage review process also achieves maximum efficiency, collaboration, and economies of scale resulting in substantial savings of public funds.

# OTF Programs

During the time period covered by this report, OTF implemented the following funds, labs, and fellowship programs.

## Funds

OTF provides direct funding to support the applied research, development, implementation, and maintenance of technologies that enable censorship circumvention and enhance user security and privacy online. OTF manages multiple funds that support innovative global internet freedom projects, large scale circumvention and secure communications technologies, and emergency support mechanisms. These funds include:

### Internet Freedom Fund

The Internet Freedom Funds the primary fund through which OTF supports innovative global internet freedom projects. IFF projects are primarily focused on technology development and implementation but can also include applied research and digital security projects.

### Technology at Scale Fund

The Technology at Scale Fund supports the large-scale circumvention and secure communication technology needs of USAGM's networks (Voice of America, Radio Free Europe / Radio Liberty, Office of Cuba Broadcasting, Radio Free Asia, and Middle East Broadcasting Networks). The fund solicits technology solutions that help deliver content to audiences in information restricted environments and protects journalists and their sources. The fund also ensures that technologies used at scale by millions of users remain secure and effective.

### Rapid Response Fund

The Rapid Response fund provides emergency support to independent media outlets, journalists, and human rights defenders facing digital attacks. The support through this fund helps these individuals and groups stay safe in repressive environments, regain online access, mitigate future attacks, and combat sudden censorship events.

## Labs

OTF provides support to existing internet freedom projects through the organization's Resource Labs (Labs). OTF's Labs provide expert services to the internet freedom community through its five Lab offerings: Engineering Lab, Red Team Lab, Usability Lab, Localization Lab, and Learning Lab. Together, these Labs provide security code audits, usability assessments, engineering support, translation and localization assistance, and secure cloud storage. These services ensure that the technologies incubated and supported by OTF are as effective, secure, and usable as possible.

### Engineering Lab

OTF's Engineering Lab helps to secure the technological infrastructure behind Internet freedom technologies. This Lab focuses on supporting the implementation and inclusion of established technologies into existing applications, organizations, and communities that are advancing Internet freedom. This includes facilitating widespread adoption of underlying circumvention and privacy technologies, supporting the infrastructure that addresses the unique needs of Internet freedom developers and end-users, and gaining better insights into the costs required to enhance existing systems.

### Red Team Lab

OTF's Red Team Lab conducts independent security audits of internet freedom technologies to help improve security of projects and ensure a safer experience for people experiencing repressive information controls online. The primary work of this Lab is reviewing and responding to issues in internet freedom software and tools.

### Usability Lab

OTF's Usability Lab improves the usability of open source circumvention and digital security technologies. This Lab supports software development teams in the creation and improvement of projects that aim to help activists, journalists, and everyday citizens communicate in privacy and security. The Usability Lab offers secure usability audits, user experience consultations, usability testing, user research and user studies, and more.

### Localization Lab

OTF's Localization Lab helps to localize internet freedom tools for different countries and regions. Addressing a major concern of the Internet freedom community of reach and adoption of technologies, this Lab helps adapt internet freedom tools that are relevant and appropriate for another country or culture.

### Learning Lab

OTF's Learning Lab helps to tell the stories of OTF-supported projects and the results they produce. Through this Lab, projects and fellows communicate the results of their projects. This Lab helps to share knowledge and outcomes with the Internet freedom community.

## Fellowships

Through OTF's research fellowship programs, OTF supports individuals that carry out cutting-edge applied research projects examining how authoritarian states are restricting the free flow of information and the ways citizens can overcome those tactics. OTF fellowships help cultivate the next generation of internet freedom experts by creating a career track for those who have the skills and passion for internet freedom.

- **Information Controls Fellowship Program (ICFP)**

  The Information Controls Fellowship Program (ICFP) supports examination into how governments in countries, regions, or areas of OTF's focus are restricting the free flow of information, cutting access to the open Internet, and implementing censorship mechanisms. ICFP cultivates the research, outputs, and creative collaboration that help mitigate threats against the ability of global citizens to exercise basic human rights and democracy.

- **Digital Integrity Fellowship Program (DIFP - FY2019 only)**

  The Digital Integrity Fellowship Program (DIFP) enables digital security experts to provide hands-on, comprehensive internet support to organizations and communities most affected by internet freedom violations (such as journalists, human rights defenders, NGOs, activists, and bloggers). Simultaneously, fellows educate the broader Internet freedom field about the threats and vulnerabilities experienced, to ensure that emerging and existing technologies best meet the needs of at-risk communities.

# History of OTF

OTF was created in 2012 as a program at Radio Free Asia (RFA), another non-profit USAGM grantee. From 2012 to 2019, the OTF program at RFA supported pioneering research, development, and implementation of cutting-edge IF technologies to respond to rapidly evolving censorship threats around the world. Today, over two billion people globally use OTF-supported technology daily, and more than two-thirds of all mobile users have OTF-incubated technology on their devices.

In recognition of OTF's success and the increasing need for the tools and technologies it supports, OTF, with support from Congress, was incorporated as an independent non-profit organization in September 2019, and was authorized under the FY21 National Defense Authorization Act (NDAA) (P.L. 116-283) in January 2021.

In April 2020, Congress allocated $20 million in funds to OTF pursuant to USAGM's FY20 Internet Freedom Spend Plan. Simultaneously, in April 2020, OTF accepted an assignment of approximately $9.8 million in ongoing USAGM-funded internet freedom contracts from RFA.

The following month, a new Chief Executive Officer (CEO) was appointed to lead USAGM, Michael Pack. Upon his confirmation, Pack immediately fired the leadership and dismissed the Board of Directors of all USAGM grantee organizations, including OTF. Pack then attempted to install new leadership at OTF and directed that all OTF's funds be frozen, preventing OTF from obligating new contracts, extending current contracts, and taking any actions related to hiring or promotion of staff. Despite significant bipartisan condemnation from Congress, USAGM, under Pack's leadership, continued to withhold $19,181,790 in congressionally appropriated funding from OTF for eight months. As a result, OTF was forced to issue stop-work orders to 49 of its 60 internet freedom projects (80 percent of all programs) in July 2020.

*"We are extremely concerned by the state of affairs at USAGM. With dangerous totalitarian regimes on the rise, including the CCP, it is essential that USAGM programs & that of their grantees like the Open Technology Fund, are up and running, and performing their vital work in accordance with their preexisting agreement with USAGM. We have given USAGM multiple opportunities to answer pertinent questions about both personnel & programming issues, but have been met with continued resistance and, at times, misleading statements, from their leadership."*

- Representative Michael McCaul (R-TX) and Senator Marsha Blackburn (R-TN)

*"The termination of qualified, expert staff and network heads for no specific reason as well as the removal of their boards raises questions about the preservation of these entities and their ability to implement their statutory missions now and in the future. These actions, which came without any consultation with Congress, let alone notification, raise serious questions about the future of the U.S. Agency for Global Media (USAGM) under your leadership."*

- Senators Marco Rubio (R-FL), Richard J. Durbin (D-IL), Lindsey O. Graham (R-SC), Patrick Leahy (D-VT), Jerry Moran (R-KS), Chris Van Hollen (D-MD), and Susan M. Collins (R-ME)

*"We are deeply concerned about the firings of qualified leadership; the reports that USAGM has frozen funds and grants; and the public reports that USAGM under Mr. Pack's leadership is considering altering preexisting budget commitments to internet freedom initiatives in order to fund products that have been subject to well-documented concerns that they do not meet technological specifications, security standards, and industry best-practices.*

- Representatives Adam Schiff (D-CA), Jamie Raskin (D-MA), Eliot Engel (D-NY), Ted Deutch (D-FL), Joaquin Castro (D-TX), Ami Bera (D-CA), Brad Sherman (D-CA), Tom Malinowski (D-NJ), David Trone (D-MD), Vicente Gonzalez (D-TX) and Dean Phillips (D-MN)

In response to Pack's actions to remove and replace OTF's leadership and Board of Directors, the D.C. Circuit Court of Appeals quickly granted OTF a temporary injunction enjoining Pack from "taking any action to remove or replace any officer or directors of the Open Technology Fund." The Superior Court of the District of Columbia subsequently granted summary judgment on the issue, confirming that Pack did not have the authority to dismiss or appoint OTF's leadership or Directors, stating that " pursuant to the plain language of OTF's bylaws... the original Board is the only valid board" and declaring that any actions taken by Pack regarding OTF's leadership to be null and void.

Despite the funding freeze imposed, OTF continued to work to deliver on its important mission by collaborating with other like-minded donors to find external support for many critical internet freedom projects impacted by the funding freeze. The organization worked with eight other like minded donors to unlock over $6 million in less than three months to support all 49 projects stopped due to the funding freeze. Because OTF was prevented from receiving any external funding and resuming project funding directly, OTF worked closely with each donor to hand off appropriate projects for them to administer and fund directly, ensuring that all 49 projects could continue operations and complete the critical internet freedom work they started with OTF.

In February 2021, a new Acting CEO was appointed to USAGM, who worked quickly with USAGM leadership to release OTF's remaining FY20 funding. As a result, OTF was able to resume normal operations and re-open all funding opportunities in March 2021. As a result of the imposed funding freeze, OTF did not finish obligating all FY2020 resources until March 2022.

# OTF Funding

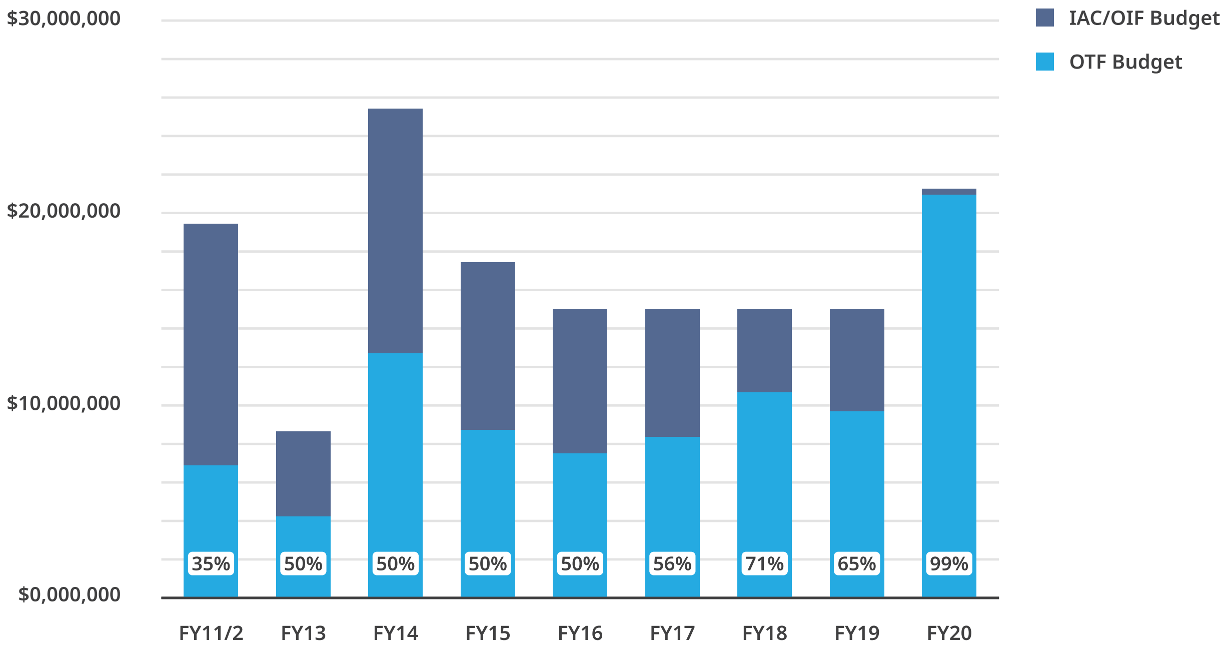
OTF is a grantee of the U.S. Agency for Global Media (USAGM) and is funded by the U.S. government through annual appropriations passed by the United States Congress to support "programs to promote Internet freedom globally." OTF's appropriations are included as a component of the Department of State, Foreign Operations, and Related Programs for each fiscal year.

Per Congressional appropriations requirements, each year, the U.S. Agency for Global Media (USAGM) submits an "Internet Freedom Spend Plan" to Congress outlining its proposed use of Internet Freedom funds appropriated in that fiscal year. The USAGM Internet Freedom Spend Plan is reviewed and approved by Congress prior to implementation.

Prior to FY2020, Internet Freedom funds allocated by Congress to USAGM were divided between OTF and USAGM's Office of Internet Freedom (OIF). Subsequent to OTF's incorporation as an independent entity, USAGM allocated the vast majority of its internet freedom funds to OTF. In FY2020, Congress appropriated $21,200,000 in Internet Freedom funds to USAGM, of which USAGM provided $21,025,000 to OTF to support internet freedom programming and $175,000 to OIF to support oversight and coordination activities.

The following graph details the recent history of USAGM Internet Freedom Funding.

### USAGM (BBG) Internet Freedom Funding History



04

# Internet Freedom Under Threat

Over the last two years, global internet freedom has come under increasing attack, with authoritarian regimes utilizing more aggressive tactics to censor content, stymie free speech online, cut access, and spread disinformation than ever before.[1] Accelerated by the global coronavirus pandemic, users in repressive environments experienced increased deterioration of their digital rights. Numerous countries have implemented regulations that curb free expression, erode privacy, and further centralize control of the internet. Even more concerning, the prevalence of internet shutdowns being used as a tool by repressive governments to silence their populations and slow the spread of truthful information has only increased.

As nations around the world saw record numbers of its citizens accessing the internet due to COVID-19 pandemic-related lockdowns,[2] global norms experienced major shifts toward greater government intervention in the digital space. This led authorities in repressive environments to expand their ability to surveil and censor information by exploiting the health crisis. Over the past two years, authoritarian governments took extraordinary measures to expand the surveillance of citizens and censorship of content websites. This included expanded censorship under the guise of safety in China, Iran, Russia, Bangladesh, Egypt, Venezuela, Cambodia, Myanmar and Belarus, among others.[3] This is in addition to dozens of governments asserting their authority over the digital collection of personal information, widespread tracking of movements and offline punishment for online activity.[4]

Alarmingly, deliberate internet shutdowns enacted by governments also increased in both frequency and sophistication. The previous two years have witnessed hundreds of internet shutdowns including in Myanmar, Syria, China, Sudan, Uganda, Nigeria, and India. While “blanket shutdowns have severe consequences and can never be justified,” the clear motivation behind many of them was s to curb political dissent, silence voices deemed harmful to local governments, and disrupt communications of those planning nonviolent discourse.[5] As journalists work diligently to share crisis information with the world, internet shutdowns have helped to hide atrocities committed by governments.[6] Furthermore, shutdowns decimate businesses that rely on internet access and have prevented the medical community from receiving vital information during the coronavirus pandemic.[7]

[1] https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech; https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123/

[3] https://freedomhouse.org/report/report-sub-page/2020/information-isolation-censoring-covid-19-outbreak

[4] https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

[5] https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

[6] https://www.accessnow.org/update-internet-shutdown-sudan/

[7] https://graphics.reuters.com/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/

Beyond the wholesale shutdown of internet access, many authoritarian governments employ internet censorship of particular platforms or websites in tandem with network shutdowns. For example, following the coup in Myanmar in February 2021, military forces enacted a series of information controls which started with intermittent outages that evolved into shutting off the internet each night while significantly increasing the blocking of online entities such as Facebook, WhatsApp and Wikipedia.[8] The 2021 elections in Uganda witnessed a similar scenario where the increased blocking of websites occurred in the lead up to the election before the government shut off the entire internet for four days on the eve of the election.[9]

Circumvention tools have also been targeted. Beyond the more common blocking of the websites of VPN and anonymity tools such as Lantern and Tor, well resourced countries have continued to escalate their efforts to limit the effectiveness of the technologies underlying these tools. The Chinese government has taken numerous steps in an effort to prevent some of the leading circumvention techniques from functioning correctly.[10] The Russian Government sought to block the use of Tor which allows users to protect their identity while accessing censored content.[11] This effort narrowed in on the most resilient techniques being relied on including the OTF-incubated Snowflake.[12] Meanwhile, the Iranian government whitelisted a small list of protocols with the goal of preventing censorship-evasion tools from functioning.[13]

This is all in addition to the targeting of communication platforms offering encryption such as Signal, WhatsApp and Telegram by countries around the globe.[14] Network throttling, whether the whole internet connection or individual platforms or websites, is also increasingly utilized. Because access is slowed but not blocked entirely it offers those doing so a greater level of plausible deniability. This tactic has been employed in many countries.[15] Perhaps the most prominent recent example was the throttling of Twitter in Russia two days after the military›s invasion of Ukraine.[16] This came months after Belarus employed a similar practice in response to widespread protests.[17]

Over the past several years, several governments have made progress building national intranets in which online traffic is limited to networks and websites operated in-country.  In November 2019, the government gradually shut off access to the internet. As they did so, they ensured access remained to locally hosted platforms that allow for robust surveillance and censorship.[18] This intranet type approach is meant to mirror what has been developed in China, who has offered to assist Iran in furthering this effort.[19]

[8] https://ooni.org/post/2021-multiperspective-view-internet-censorship-myanmar/

[9] https://ooni.org/post/2021-uganda-general-election-blocks-and-outage/

[10] https://gfw.report/

[11] https://ooni.org/post/2021-russia-blocks-tor/

[12] https://www.wired.com/story/tor-browser-russia-blocks/ ; https://www.opentech.fund/about/people/serene-han/

[13] https://geneva.cs.umd.edu/posts/iran-whitelister/

[14] https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/

[15] https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/

[16] https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/#twitter-throttled; https://censoredplanet.org/throttling

[17] https://www.engadget.com/twitter-belarus-blocking-protests-194657126.html

[18] https://www.article19.org/ttn-iran-november-shutdown/ ; https://ooni.org/post/2019-iran-internet-blackout/#irans-intranet

[19] https://www.rferl.org/a/iran-china-national-internet-system-censorship/30820857.html

The Government has subsequently utilized this tactic repeatedly during times of unrest.[20] While Iran has claimed the "National Information Network" will be completed in 2025, the capabilities demonstrated to date highlight both the advances in a project started in 2013 and the severe economic consequences of utilizing it.[21]

The Russian government has undertaken a similar scheme. Following the passage of a "sovereign internet" law in late 2019, a series of nationwide tests have allowed continued refinement of the effort.[22] The technology underlying this was multi faceted. The national DNS system maintains a localized copy of the wider internet and was the focus of these tests. The plan also gave the government expanded capacity to implement other information controls such as the throttling of Twitter mentioned previously.[23] This is a result of centralizing control for the implementation of censorship to limit the impact of the fragmented market for ISPs. This upgraded equipment provides Russia's internet regulator, Roskomnadzor, additional mechanisms to interfere with users' access and reduce privacy.[24] This is, of course, in addition to the Russian governments escalating pressure on platforms, app stores and other players in the online ecosystem.[25]

As a result of the rise of the private surveillance industry and COVID-19 pandemic-related surveillance policies, large-scale digital surveillance has increased astronomically over the past two years, posing a significant threat to freedom of expression, independent journalism, democracy, security, and human rights globally. New technologies, including machine learning and the precursors to artificial intelligence, have enabled faster, more accurate, and more targeted surveillance at unprecedented scales. Once only available to a small number of well resourced regimes, highly advanced surveillance technologies are now widely accessible to nation-states and other non-state around the globe. Today, any government with an interest in surveilling its citizens can easily acquire the tools necessary to conduct near real-time mass surveillance. Widespread revelations have occurred demonstrating the extensive misuse of Pegasus, the chief product sold by the NSO group. While this is only one actor in the surveillance industry ecosystem, the ubiquity of its usage aptly demonstrates the runaway nature of this industry and the resulting harms.[26] The pervasive use of increasingly sophisticated digital surveillance and censorship technology by authoritarian regimes has left civil society more vulnerable than ever.

[20] https://www.haaretz.com/middle-east-news/2022-05-31/ty-article/.premium/iran-cuts-internet-as-protest-erupts-over-deadly-tower-collapse/00000181-1a87-dfc2-a9a1-ffdf2a2c0000

[21] https://developingtelecoms.com/telecom-business/telecom-regulation/11816-iran-eyes-2025-to-complete-controversial-national-intranet.html

[22] https://www.bbc.com/news/technology-50902496

[23] https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22/

[24] https://www.wired.com/story/russia-splinternet-censorship/

[25] https://time.com/5951834/russia-control-internet/

[26] https://citizenlab.ca/tag/nso-group/

05

# Project Highlights

During the period covered by FY2019 and FY2020 funding, OTF funded over **70 innovative projects** to combat censorship and repressive surveillance. It supported **13 fellows** to engage in cutting-edge research and digital security interventions. It also funded **5 labs** to improve the security, usability, resiliency, and interoperability of key internet freedom technologies, and over **30 rapid response interventions** to address digital emergencies.

A full list of all supported projects is included at the end of this report. This section provides an overview of key project highlights.

## Combatting Censorship

While authoritarians have become far more adept at using the internet to control information, the internet is still far and away the medium through which most information reaches audiences in highly restricted information contexts. To a first approximation, the contemporary samizdat is an entirely online phenomenon. Equipping citizens of authoritarian states with the tools and technologies they need to access objective, global news and information, despite their governments' attempts to restrict access to such information, is core to OTF's work.

Over the past two years, OTF has continued to fund an increasingly robust and sophisticated suite of network measurement technologies that has enabled technologists, activists and journalists to track in real time the evolution of censorship techniques and targets across the globe. With funding from the period covered by this report, the Internet Outage Detection & Analysis project (IODA), which documents and verifies instances of politically-motivated interference with internet access, increased the accuracy and breadth of detection and made its platform more useful and accessible to non-technical users. This proved vital in tracking specific regional internet outages in Ukraine following the Russian invasion. Investments in the Open Observatory of Network Interference (OONI) improved the monitoring of website censorship, expanded the breadth of global coverage and granularity of censorship events, and empowered community participation in censorship measurement research. This allowed testers in the weeks after the invasion of Ukraine to chart the rapid evolution of Russian censorship of ISPs and allowed digital security practitioners to respond in a quick and informed manner.  Funding to Netalitica during this period also improved the data OONI relies upon for maximum testing efficacy.

The challenge of circumvention in the context of the contemporary internet is defined by the growing sophistication of censors and the diverse needs and technical aptitudes of users. Over the past two years, OTF invested substantially in a range of trusted, intuitive anti-censorship tools appropriate for contexts of various users while also keeping technical pace with the most sophisticated global censorship tactics. Support for VPN-style circumvention tools such as Psiphon, Lantern and NthLink have provided direct circumvention life-lines to tens of millions of users in censored countries from Cuba to Belarus to Myanmar, particularly in periods of political and social unrest. In addition to these large-scale circumvention tools, OTF has also supported the development of new circumvention technologies for high-risk use cases. The first is MassBrowser, a technology through which users in uncensored areas serve as bespoke circumvention proxies for users in censored areas. The second is oLink, a censorship circumvention tool that does not require any software installation and allows users to access blocked content from a standard web browser by mirroring blocked sites in a way that is difficult to censor.

In addition to supporting circumvention tools themselves, OTF has also invested in improving the state-of-art of circumvention more broadly. OTF support for Wireguard fundamentally improved the VPN landscape, as Wireguard's far simpler and more secure protocol now makes it far easier to debug and secure compared to standard VPNs and has, by default, raised the security posture for millions of internet users globally in the background without any additional action on their part. The WireGuard protocol's state-of-the-art cryptography and lightweight 4,000 line code base has consistently proven to be easier to set up and securely maintain than existing options, such as IPsec or  OpenVPN. Unlike other popular VPN protocols, which can have over 100,000 lines of code that must be monitored and debugged in order to be secure, WireGuard provides security through the most lightweight codebase possible. As a result of these integrations, WireGuard is now used by over a billion people worldwide.  In addition, OTF support for DEfO, and its component Tolerant Networks Limited (TN), provided client and server-side support for Encrypted Server Name Indication (ESNI) in OpenSSL. Encryption of SNI values provides a way to circumvent the blocking of specific websites, and has made it easier for users to navigate the open internet.

During this period, OTF also supported new efforts to reduce the cost and increase the efficiency of circumvention efforts by investing in new machine-learning techniques. In order to meet the resources imbalance between highly resourced nation-state censors and far less resourced internet freedom tech developers, OTF has invested in technologies that leverage AI to automate the discovery of censorship evasion strategies without the need to hypothesize and build them first. Geneva, a genetic algorithm that has trained against real-world censors in China, India, Iran, and Kazakhstan to automatically identify new censorship techniques and evasion strategies. To date, the tool has discovered dozens of previously unknown strategies to defeat state-level censorship.

# Mitigating Internet Shutdowns

Until recently, the common belief was that internet shutdowns were too costly, both politically and economically, to be deployed by governments as a means of controlling information on a national scale, with routine frequency, or for reasons less than the politically existential. This assumption has been completely and categorically disproven by numerous politically motivated shutdowns of a previously unthinkable size and scale, perpetrated by regimes that bore the associated costs and normalized a new form of control. It is no longer just specific content that is subject to censorship, it is the flow of data itself. In addition, similar to more traditional forms of censorship, "shutdowns" now take many forms that necessitate highly context-specific solutions.

One form of internet shutdown -- exemplified by Iran's National Information Network – is a shutdown in which national communications infrastructure remains functional but is cut off from all points of global connectivity presents several avenues for meaningful mitigation. OTF support for Ouinet has created peer-to-peer content distribution networks that can serve a variety of cached content to users within areas cut-off from global networks. The former via its CENO Browser is already deployed in some of the world's most shutdown prone areas such as Iran and Myanmar while the latter has already been integrated into USAGM newsreader apps. In addition, OTF-supported Delta Chat leverages an email backend and encryption to create an adaptable, decentralized secure messenger that enables privacy features and resilience to interception that is vital for users in repressive contexts even if only national email servers are available. Delta Chat is available for download and use everywhere on Apple and Android devices.

Another form of shutdown - illustrated by the Junta in the days following the military coup in Myanmar – is to shutdown the internet and mobile data but allow cellular calling and SMS in order to drastically restrict the flow of information but allow some basic communications to continue. While this may be preferable to a total network shutdown, many of the communication functionalities and security securing messaging apps are lost. OTF support to Frontline Local and additional investments that build off that foundation attempt to extend some of the functionality and security guarantees of secure messengers to SMS-based communications for these types of shutdown situations.

Finally, OTF is also supporting the development of tools for total network shutdowns. In addition to offline device-to-device messagers, During the period covered by this report, OTF also supported Awala (formerly Relaynet) to create a technology whereby human couriers with an app can securely and privately collect data to be sent from areas without connectivity. When the couriers move physically to a connected area the data is automatically transmitted and then data received in response can be transported back into the disconnected area where it automatically syncs with the original senders - in effect physically carrying bursts of vital connectivity into completely disconnected areas.

# Increasing Security

As authoritarian regimes frequently enact offline reprisals for online activities, security and privacy online have become necessary preconditions for exercising the right to free expression online in many repressive countries. As a result of these stakes as well as the increasing availability of technically sophisticated surveillance technologies to authoritarians on any budget, OTF invests in improvements to the overall security of the internet and supports the development of tools for the specially most targeted users. Seeking to mitigate a common vector for man-in-the-middle attacks, OTF support helped develop a more secure domain validation protocol known as multiple vantage point domain validation (MVP-DV). According to the Electronic Frontier Foundation OTF's support to implement this protocol into Let's Encrypt "helped protect the 227 million sites using Let's Encrypt from BGP attacks, a favorite technique of nation-states that hijack websites for censorship and propaganda purposes." In this report period, the DL-ISAC project further modernized and extended DDoS protections to hundreds of civil society and journalistic sites. Building on novel vulnerabilities discovered through William Tolley's ICFP fellowship, Breakpointing Bad revealed inherent flaws in VPN's security and privacy properties and educated vulnerable populations about the flaws of VPN technology, disclosing to necessary parties all vulnerabilities found, and examining potential fixes for VPN issues. In recognition of the surveillance risks posed by IMSI-catchers, which pose as fake cell phone towers, the FADE Project expanded studies to detect the use of IMSI-Catchers in a standardized way in Latin America to further develop the detection methodology, technical tools, and mitigation strategies for the civil society actors and journalists in the region.

# Advancing Research

Research plays a crucial role in protecting internet freedom. It informs frontline defenders about the developing threat landscape, identifies new challenges on the horizon, and supports the development of novel internet freedom tools and ways to improve existing ones. OTF supported a number of researchers working on the urgent threats to Internet freedom identified above. These applied research projects supported through OTF's Internet Freedom Fund and its Information Controls Fellowship Program provide direct feedback, insight, or applicability to technology development processes. This research includes how, why, or where censorship is happening or understanding how the threat of targeted surveillance is evolving across the globe and how we can fight back against it. It also includes developing new methodologies for studying Internet freedom, for instance through applying machine learning techniques, to advance knowledge around what types of content censors target and how they do so, or assessing threats to Internet freedom in a specific geographic context through on the ground research.

OTF continues to lead the field in internet freedom research by supporting expert researchers through its Information Controls Fellowship Program (ICFP). During the report period, OTF supported its seventh and eighth classes of ICFP fellows. Fellows conducted research on a variety of critical topics related to internet censorship, including techniques to identify and monitor censorship technologies, investigations into the underlying mechanisms used to identify and block censorship circumvention protocols, and understanding and centralizing internet shutdown data.

For example, with OTF support, researchers developed a measurement platform that continuously monitors the Chinese government's DNS filtering mechanism and identifies changes to censorship tactics over time. In addition, OTF-supported researchers developed computational methodologies to better identify and analyze internet shutdowns. Researchers also investigated DNS-poisoning, the role of ISPs in internet shutdowns, website encryption, interference with VPN connections, and new circumvention techniques.

### Investigating Internment Camps in Xinjiang

OTF supported an investigation of the internment camps in Xinjiang, which was published in late 2020. The investigation behind this report began when researchers noticed that blank tiles appeared in the Chinese mapping platform, Baidu, in the vicinity of known internment camps in Xinjiang. When the researchers confirmed that they could replicate this phenomenon reliably and that it happened in multiple camp locations, they used the technique to locate the rest of the camp network. When the investigation began, it was believed that there were around 1,200 camps in existence, while only around 70 had been located. Through this investigation, researchers discovered that there has been a shift in the internment program and that, since 2018, the Chinese government has been building a series of much larger, more permanent, and heavier security facilities. Using this technique, OTF-supported researchers were able to locate 268 new compounds believed to be a part of the current program, many containing several camps and prisons, and a wider network of 428 compounds.

### Auditing TikTok

In 2020, OTF supported an ICFP fellow to conduct a security, privacy and censorship audit of TikTok, a short-video sharing social media app popular among young internet users. ByteDance, a China-based technology company develops TikTok, a video-based social media platform which is the first Chinese-made social media platform that reached global popularity, crossing 2 billion accumulated downloads in April 2020. The app started in China under the name Douyin, and was released as TikTok tailored for the international market. Despite TikTok's popularity and prominent public discussions surrounding its security and privacy, neither TikTok nor Douyin have been thoroughly studied. The ICFP fellow worked closely with Citizen Lab at the University of Toronto to carry out research on the technical characteristics of TikTok and Douyin through analysis of the source codes of TikTok and Douyin's Android apps.

### Understanding Censorship in Burma

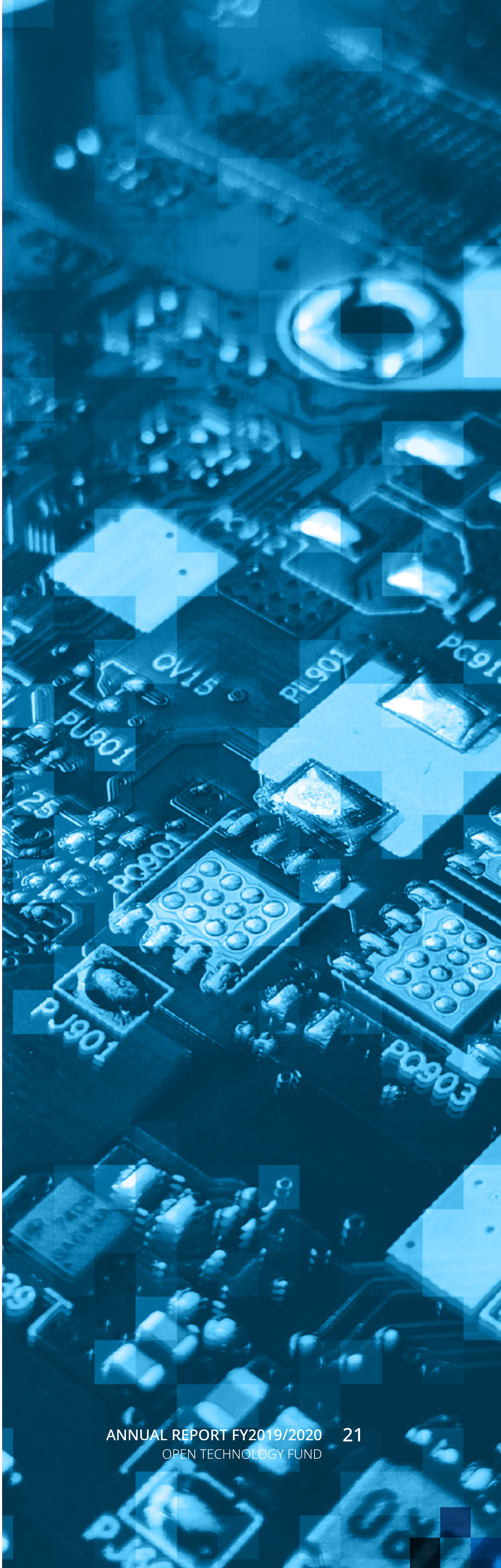
In November 2020, an OTF Research Fellow published The Rise of Online Censorship and Surveillance in Myanmar: A Quantitative and Qualitative Study, a comprehensive analysis of the various surveillance and censorship tactics currently in use by the authorities in Myanmar in an effort to shine a light on this otherwise opaque system. Their research focused not only on the specific technologies in use in the country, but also on the offline spaces and legal loopholes which can inhibit transparency and allow government and military officials to implement surveillance and censorship practices in an unchecked manner. The research indicated that the Myanmar government made significant investments in surveillance technology. Further, the vast majority of interviewed human rights defenders, journalists, and others working on sensitive issues reported not feeling secure online.

### Assessing New Circumvention Techniques

Another OTF ICFP Fellow worked with the University of Waterloo to assess the viability of a new censorship circumvention technique that supports low-latency proxying and redundant file storage, both with plausible deniability. This mechanism has the potential to address various tactics used by modern censors, such as protocol fingerprinting, traffic analysis, Internet shutdowns, and bridge enumeration attacks. The ICFP Fellow also developed a prototype implementation during the fellowship.

### Analyzing Censorship and Circumvention in Africa

In September 2020, an OTF Research Fellow published Censored Continent, examining the use of internet censorship circumvention tools in Cameroon, Nigeria, Uganda, and Zimbabwe, four countries in Africa with varying degrees of censorship, including bandwidth throttling, social media app restrictions, and website blocks. Their research is helping to inform the dissemination of important internet freedom tools in those countries.



# Responding to Digital Emergencies

Over the two years, OTF has successfully responded to numerous acute digital threats through the rapid response fund with projects in Belarus, Burma, Cuba, Ukraine, and Russia, among others.

## Belarus

In August 2020, pro-democracy protests broke out in Belarus. In response, the government quickly implemented aggressive internet controls, including increased internet censorship and surveillance. Despite restrictions on OTF's funding and operations at the time, OTF still worked to provide internet freedom support – albeit limited – to civil society in Belarus. To support journalists and democracy activists in Belarus to overcome new internet restrictions, OTF provided critical digital security support to civil society groups; funded secure hosting and cyber-attack mitigation platforms; and supported cutting edge network monitoring efforts to better understand, and ultimately overcome, censorship in Belarus. In addition, even with limited resources, usage of OTF-supported tools, including Psiphon, Tor, and Signal, spiked dramatically in response to the government's crackdown. After the Belarussian government announced that they had blocked all RFE/RL websites, OTF worked quickly with RFE/RL to spin up several mirror sites so that RFE/RL audiences in Belarus could continue to easily access their websites and content free from censorship.

## Myanmar

In February 2021, military leaders seized control of the government of Burma and declared a state of emergency. After the coup, the military quickly increased internet censorship, including several short-term internet shutdowns. OTF's research partners closely monitored the censorship situation in Myanmar after the coup and were the first to identify and report the shutdown. In addition, use of OTF-supported circumvention tools increased rapidly after the coup - from several thousand to millions of users in just a matter of weeks. At the peak, OTF-supported circumvention tools were being used by over 6 million monthly users - over 10 percent of the country's population. These tools were not only critical in enabling citizens to access and share information, they also enabled VOA and RFA to continue reporting and reaching their audiences. In fact, despite being blocked by the military, VOA's Burmese website broke its record of website visits in a single day, with just under 1.3 million visits, via OTF circumvention tools. In addition, OTF supported numerous rapid response projects to provide emergency digital security training and cyber attack mitigation assistance to independent journalists and local civil society organizations.

## Cuba

Similarly, in July 2021, the Cuban government blocked several popular social media sites and messaging applications in response to civilian protests. As a result, use of OTF-supported circumvention tools skyrocketed from several thousand users to roughly 1.5 million users in a matter of days - the highest number of circumvention tools users ever recorded in Cuba.

## Ukraine

The Russian government invaded Ukraine in February 2022. Given the Russian government's known offensive cyber capabilities, experts predicted that the Russian government would attempt to immediately surveil and/or shut down internet connectivity in Ukraine upon its invasion of the country. While a shutdown has not occurred to date, Ukrainian citizens have taken proactive steps to protect themselves from digital threats. For example, in the wake of the invasion, Signal - an OTF-supported secure communication tool - was the most downloaded and most used messaging application in Ukraine, exceeding even Telegram. In addition, adoption of OTF supported-circumvention tools has increased significantly despite the lack of censorship, likely driven by concerns of potential Russian government surveillance. Further, OTF has worked with local partners to deploy shutdown resistant technologies in anticipation of potential Russian government imposed internet shutdowns. For example, OTF has helped deploy infrastructure that will allow Ukrainians to access the internet from regional points of connectivity despite physical infrastructure damage in other regions, and access content in a peer-to-peer fashion should the national internet be cut off by the Russian government.

## Russia

Following the invasion of Ukraine, the Russian government dramatically increased censorship efforts, targeting independent news sites (including RFE/RL and VOA) and social media platforms in particular. In response, use of OTF-supported circumvention tools has surged dramatically, increasing from a few thousand users pre-invasion to nearly 2 million daily users. In addition to VPNs, OTF-supported mirror sites have received hundreds of millions visits. As a result of these efforts, visits to RFE/RL's websites tripled compared to pre-invasion traffic, and have since stabilized to over 150% compared to pre-invasion traffic. Content on social media has also had significant spikes in traffic, demonstrating that OTF-supported circumvention tools are successfully enabling Russian citizens to circumvent censorship and access USAGM content.

# Community Solidarity

One of the most disturbing trends across the internet freedom landscape today is the way in which authoritarian regimes are sharing technological approaches to surveillance and censorship all while normalizing such repressive internet restrictions. It is therefore vital that internet freedom advocates and technologists share information and technical solutions to keep pace. Community coordination is the vital connective tissue that ensures internet freedom practitioners are not fighting highly resourced adversaries in isolation.

In coordination with the State Department's Bureau of Democracy Human Rights and Labor, OTF supports the Internet Freedom Festival (IFF), one of the biggest Internet Freedom gatherings in the world that brings together activists, journalists, developers, humanitarian workers and others working on freedom of expression, privacy and security. To address the deterioration of community ties and health of internet freedom networks during the pandemic, OTF's support helps the IFF to create and maintain trusted spaces for internet freedom groups to share knowledge and pool resources, ensure at-risk voices are included, and assess and preempt post-COVID challenges.

OTF complemented broad community coordination efforts with more targeted support including for Bread & Net a vital MENA regional Internet Freedom forum, support for TibCert to create a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community including a research focus on understanding how surveillance and censorship work at specific points where Tibetans are targeted via device and app stores vulnerabilities. OTF also extended its substantial technology localization efforts to indigenous communities under threat by mapping and documenting the language-related challenges facing localization in the adoption and safe use of internet freedom technologies, particularly as it relates to existing networks of front-line digital activists from dozens of communities working in under-resourced languages.

In addition to serving the needs of the broader internet freedom community, OTF held its seventh summit in January 2021. Due to the COVID-19 pandemic, the summit took place online. In recognition of the internet freedom community's resilience in the face of unprecedented and escalating threats to internet freedom, the theme of the summit was Solidarity. To reflect this theme, the summit's sessions focused on discussing and exchanging learnings on building resilience and overcoming shared challenges.

# Increasing Need

In the context of a rise in global surveillance and in the wake of acute, politically-motivated censorship surges, the demand for secure, robust and trustworthy anti-censorship tools has skyrocketed. In response, OTF has both increased and diversified support to globally effective circumvention tools, which now support tens of millions of users in some of the world›s most censored places including China, Iran, Burma, Russia, Ukraine, Belarus, Cuba, and Ethiopia. OTF-supported tools have proven technically robust in the face of even the most advanced and unanticipated attempts to censor news and information, ensuring that users in crisis were not cut off from the outside world. Building off their technical successes, OTF is now attempting to optimize support for these tools in light of their huge and sustained user populations. Even as OTF strives to develop new solutions to stay ahead of increasingly sophisticated adversaries, it is also vital that current user populations are supported and maintained.

The Islamic Republic of Iran
Has shut down the Internet
It doesn't matter if you are Iranian or not.
If you believe in Human Rights, please be our voice

# 06 Direct Support with FY2019 Funds

## Internet Freedom Fund (FY2019)

The Internet Freedom Fund (IFF) is the primary fund through which OTF supports innovative global internet freedom projects. IFF projects are primarily focused on technology development implementation, but also include applied research and digital security projects. OTF continuously solicits IFF project proposals through a fully open, transparent, and competitive process.

### Delta Chat

**$299,790**

Delta Chat is a unique messaging application that combines modern messaging user-interface paradigms with an e-mail backend, enabling end-to-end encryption with Autocrypt, a mobility security provider. The project leverages such e-mail encryption to create an adaptable, decentralized secure messenger that enables privacy features and resilience to interception that is vital for users in repressive contexts, and can be safely used by journalists, activists, organizers, and the general public. By addressing the needs of frontline activists who are exposed to asymmetric threats, Delta Chat improves secure access to messaging applications when the internet is restricted or surveilled.

### Azerbaijan Internet Watch

**$87,410**

Azerbaijan has taken an unprecedented downward trend in the restriction of information and violations to freedom of speech over the past five years. While Azerbaijani internet was once the predominant space for dissent, alternative mobilizing, activism, and a source for information, the government has stepped up their attacks against information sharing, online activists, and digital media outlets. The goal of the Azerbaijan Internet Watch project is to examine how relevant institutions in Azerbaijan restrict information and deploy censorship mechanisms that violate access to information and freedom of speech. This project helps address the large information gap that exists around critical developments related to internet freedoms in Azerbaijan by monitoring internet censorship, measuring and classifying digital attacks, and raising awareness on digital crackdowns among the general population. The project looks into blocked websites, DDoS attacks (distributed denial-of-service) that disrupt normal traffic to a legitimate website, hacking attempts, shutdowns, blackouts, spear phishing, surveillance, and physical arrests for online actions.

## PiGuard

## $72,830

Virtual Private Networks (VPNs) are widely used by activists, bloggers, and journalists to secure online communication and circumvent censorship. However, it is increasingly easy for governments and ISPs (internet service providers) to shut-down a service simply by blocking the IP address of the server providing the VPN service. The PiGuard project utilizes WireGuard's "IP Roaming" feature, which allows a device to automatically connect to a new VPN server in case the previous server was blocked. This project embeds WireGuard in smaller, more affordable servers to create WiFi hotspots that allow connected users to benefit from an encrypted connection. By creating this WireGuard VPN infrastructure, PiGuard increases the digital safety of journalists and human rights defenders on the grassroots level with easy-to-use circumvention technology.

## **Relaynet** (known as Awala in FY2020 and beyond)

## $127,757

Relaynet (now Awala) is a decentralized computer network where compatible applications use the Internet when it is available (i.e. normal internet access) and switch to a backup medium when the Internet has been cut off. The decentralized network works by distributing information across multiple devices instead of relying on a single central server to communicate information. This technology was designed to circumvent complete internet blackouts caused by repressive regimes, enabling users to communicate with one another even when traditional access is down. Data is transported using storage devices, WiFi, Bluetooth, and mesh networks, with the user only needing an application that supports Relaynet and a Relaynet gateway, which is a server running locally on their computer or smartphone. OTF's support helped implement the core of the technology on desktop and Android developments and enhance safety features.

## **5G and Human Rights:** The Societal Risks of Network Virtualization and Autonomation in New Digital Communication Infrastructures

## $129,810

5G networks, the fifth generation technology standard for broadband cellular networks, continues to be deployed around the world. The widespread adoption of 5G will have a significant impact on the flow of data streams and the information architecture, altering how information is sent, filtered, routed, as well as the parties that have access to it. This project analyzes the risks and opportunities of 5G for human rights, freedom of expression, and the right to privacy. The associated research focuses on Brazil and South Africa, both countries where human rights are under severe threat where 5G is being implemented. The project also aims to identify and communicate ways to mitigate negative impacts.

## Cupcake

## $12,500

Cupcake is a web browser extension that lets uncensored users contribute their own internet access to create new entry points to the Tor network. Tor is an open-source software for enabling anonymous communication. Cupcake benefits at-risk individuals who are not able to connect to the internet through the Tor network's more traditional introduction points, such as guard nodes and bridges. For most users, connecting through this method offers a more robust defense against a wider variety of surveillance and censorship threats.

## Secure UX Design Method

## $250,601

The Secure UX Design Method is a methodology and taxonomy designed as a "how-to guide" for researchers, engineers, product managers, designers, and teams. The project aims to provide a series of actionable best practices and guidelines for those who build tools for and with marginalized communities, from the ideation stage to the finished product stage. The project features curricula and an accessible website that teaches people about design and security in plain terms. Included among the curricula are educational resources like a glossary, short videos, screenshots of good and bad practices, questionnaires, short quizzes, as well as written descriptions and explanations.

## FrontlineLocal

## $250,000

The growing use of internet shutdowns by repressive governments to stifle dissent and limit access to information has added another critical layer of insecurity for politically and operationally vulnerable organizations. These governments censorship methods and shutdown capabilities have gotten more sophisticated in recent years, going so far as to compel mobile network operators and internet service providers to shutdown connectivity at key moments. For most people, security and circumvention tools rely on the internet, and without internet access, many organizations lack the tools to maintain communications or access information. FrontlineLocal is a hybrid messaging management platform that enables users to safely and effectively communicate using SMS during network shutdowns. The tool allows users to manage and automate SMS communication to distribute information, such as high-priority news and alerts.

## Improving Lists of Censored Online Content

## $161,518

In measuring internet censorship, test lists are an important tool to determine which websites may be blocked on a network. However, for many highly censored states, the entries on these test lists have seen few updates over the years, leading to poor quality of collected measurements. These include, for example, URLs that lead to dead websites or domains that have been sold or redirected to irrelevant content. The mechanisms for updating these lists have barely evolved, which deters volunteers from participating in the update process. This project updated the lists of 28 countries in Latin America, Asia, Africa, and the MENA region. Additionally, the project improves the methodology for maintaining lists by involving local organizations in the updating process and developing a user-friendly intake form to ease the process of updating the lists.

## Reveal

## $198,939

The development of censorship and surveillance techniques in North Korea are not as well understood as other repressive governments with well known information controls, such as China and Iran. This project seeks to detail all the methods employed by the North Korean government to prevent the free flow of independent information by reverse engineering North Korean smartphones and other devices to discover and detail the methods used by the North Korean government to prevent the consumption and sharing of information between users. In addition, the project will create a development history to better understand the way censorship technology in North Korea has evolved over time to better understand the direction that such development is heading, as well as the limits and trade-offs North Korean authorities are faced with in their attempts to develop a system of digital control and repression.

### Smarter Test Target Selection & Analysis for Global Censorship Monitoring

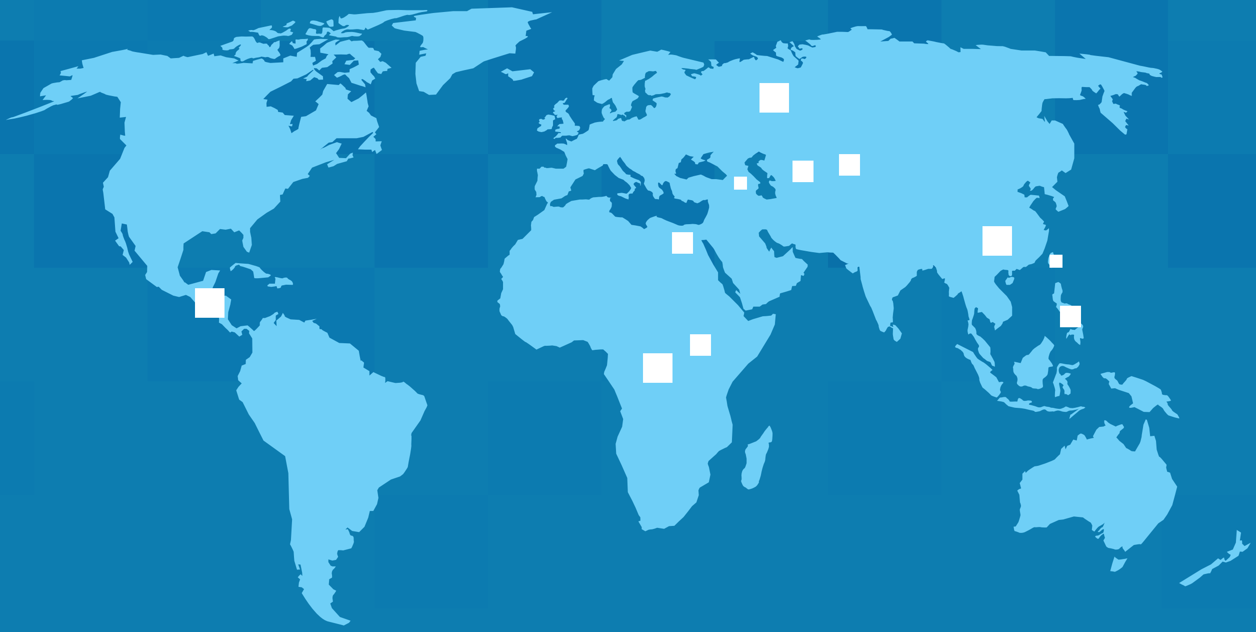
**$425,880**

Measurement tools are critical to recording and ultimately overcoming the rapid growth of censorship and surveillance that impedes free expression and violates civil and human rights. This project, conducted through the Open Observatory of Network Interference (OONI) significantly advances both the capabilities and proliferation of the platform to better enable the internet freedom community to rapidly respond to censorship events in promotion and protection of human rights and democracy. With OTF's support, this project improved the monitoring of website censorship, expanded the breadth of global coverage and granularity of censorship events, and empowered community participation in censorship measurement research.

### Dark Crystal

**$161,270**

While modern encryption techniques are strong, they are rarely used by those who need them. A recurring reason for this is users' fears of losing access to critical data. Data storage mechanisms, such as privately owned offline storage, virtual private servers, reliable cloud service, and more have their own intrinsic limitations. Additionally, while traditional forms of data backup make more sense for sensitive media, they are less suitable for personal cryptographic keys. Dark Crystal is a protocol for distributed data persistence and threshold-based consensus, providing a toolkit for developers of applications where effective management of sensitive data is critical. This includes a protocol for distributed backup and recovery of cryptographic keys, an implementation in Java, and a comprehensive guide to the techniques. The aim of Dark Crystal is to make sharding technology (the method for distributing a single dataset across multiple databases) intuitive and accessible to developers, and ultimately the end-users of existing applications.



# Rapid Response Fund (FY2019)

OTF's Rapid Response Fund (RRF) provides emergency support to independent media outlets, journalists, and human rights defenders facing digital attacks. The support through this fund helps these individuals and groups stay safe in repressive environments, regain online access, mitigate future attacks, and combat sudden censorship events.

In 2019, OTF facilitated timely and comprehensive emergency responses around the world. OTF provided secure hosting, security audits, website sanitation, and more to civil society organizations while also providing direct funding for in-country internet freedom support. OTF's Rapid Response support is global, and has supported activities in El Salvador, Uganda, Uzbekistan, Russia, Philippines, Egypt, Kyrgyzstan, Armenia, Guatemala, and more.

# Labs (FY2019)

OTF provides support to existing internet freedom projects through the organization's Resource Labs (Labs), which aid the internet freedom community in tackling the diverse nature of challenges posed by repressive regimes and authoritarian governments. These resources assist the relatively common needs for tools and technologies operating in this space, and include items such as secure hosting, code audits, communications and localization assistance, usability design, and more. OTF's Labs provide these expert services to the internet freedom community through its five Lab offerings: Engineering Lab, Red Team Lab, Usability Lab, Localization Lab, and Learning Lab. These services ensure that the technologies incubated and supported by OTF are as effective, secure, and usable as possible.

## Engineering Lab

The Engineering Lab focuses on supporting the implementation and inclusion of established technologies into existing applications, organizations, and communities that are advancing internet freedom, supporting the operating and infrastructure costs associated with tool and resource deployment, and conducting assessments of existing apps or websites for recommended privacy, security and anti-censorship improvements. This Lab's service offerings are provided by Greenhost (eclips.is), Throneless Tech, Maxwell Pearl, Combonet, Guardian Project, Mullvad, and Private Internet Access.

Despite the challenges faced in 2020, OTF was able to provide crucial support services through the Secure Cloud initiative Eclips.is. This support has proved to be a vital resource for OTF projects and the broader internet freedom community by providing a secure development space for new tools and technologies, including hosting web-based access to control project resources on the cloud.

### Eclips.is (Greenhost)

**$330,058**

Eclips.is (formerly Greenhost) is a secure cloud resource and a vendor for OTF's Engineering Lab. Eclip.is has emerged as a vital resource for OTF projects and the internet freedom community, helping to manage secure cloud computing infrastructure and web-based platforms for those seeking support through the Engineering Lab. Eclips.is is one of the Engineering Lab's primary service partners.

## Red Team Lab

The Red Team Lab offers services that look to strengthen the security of open-source internet freedom software by providing security audits, advancing projects' software security best practices, validating privacy and security claims of projects, and more. By focusing on improving the software security of projects that advance OTF's internet freedom goals, supported projects can ensure that the code, data, and people behind each project have the tools they need to create a safer experience for those experiencing repressive information controls online. The work of this lab is primarily reactive by reviewing and responding to issues in pre-existing software, and is supported by the Lab's service partners Cure53, Include Security, Radically Open Security, Subgraph, NCC Group, and HackerOne.

During the time period covered by FY2019 funding, OTF's Red Team Lab provided critical support for internet freedom projects serving both those in repressive regimes and the broader internet. One such example is Monocypher, which worked with the Red Team Lab service providers to improve cryptographic code needed to build the privacy and security oriented applications provided by the Monocypher library. Another, Flowcrypt, utilized the Lab to make email encryption more accessible to non-technical users, educators, NGOs, non-profits, and more. The Lab's work also crossed language barriers, such as supporting the user access and digital security technology of Zanga, an Arabic language app store for circumvention, privacy, and digital security tools.

### NCC Group Security Services

### $150,000

NCC Group Security Services is a global cyber and software resilience organization operating across multiple sectors, geographies, and technologies. As a Red Team Lab vendor, NCC helps OTF and its projects by providing detailed professional reports of the findings and recommendations from security audits of programming code and penetration tests of systems. By establishing a high-level of privacy and security standards, NCC conducts independent technology audits, network penetration testing, code audits, recommended solutions for gaps and vulnerabilities, reference materials used to support findings, and more.

### Radically Open Security

### $50,000

Radically Open Security, a non-profit computer security consultancy, aids OTF as a Red Team Lab vendor by providing professional audits of programming code, penetration testing of systems and networks, organizational and operational security training, and providing detailed reports on findings alongside recommended solutions. Radically Open Security's unique non-profit business model supports transparency, openness, and giving back to the community.

### Subgraph

### $50,000

Subgraph is an open source security company with specialized experience in application security. As a Red Team Lab partner, Subgraph supports the security needs of OTF-supported projects and projects from the broader internet freedom community through security audits and penetration testing based on well-established principles from the security and cryptography industries.

## Community Lab

The Community Lab provided services that empowered the community to become strong and vibrant by focusing on cultivating deeper trust relationships, improving knowledge share and collaboration, and supporting and diversifying the next generation of leaders. OTF supported the internet freedom community, global and cross-cultural by nature, by helping the community build spaces that empower individuals to network, address existing and emerging needs and opportunities, share resources and knowledge, and collectively strategize.

### Public Internet Infrastructure Workshop

**$25,160**

In FY2019, OTF supported ARTICLE19, a public internet infrastructure workshop that aimed to build and strengthen the relationship between researchers and practitioners in order to improve the efficacy of civil society engagement in standards setting fora in order to critically contribute to the development of rights-enabling internet infrastructure. The two-day hands-on meeting brought together 30 scholars, technologists, and practitioners to discuss how to ensure that the internet infrastructure serves the public interest.

## Localization Lab

The Localization Lab addresses a major concern of the internet freedom community in tool-localization by helping to cut delays in making internet freedom tools relevant, appropriate, and available for individual countries and cultures. Often limiting the broad adoption of a critical tool, localization supports efforts to provide tools in a given user's native language and expanding the reach of OTF-funded projects.

## Usability Lab

The Usability Lab (now the Secure Usability and Accessibility Lab) offers secure usability and user-interface assistance to internet freedom and digital security tools to help them recognize and solve usability challenges that hampered the adoption of those tools in repressive contexts. OTF partners with service providers that offer secure usability and accessibility coaching, consultation, and audits that help the advancement of the internet freedom community and the accumulation of practical knowledge through peer-to-peer learning.

## Learning Lab

The Learning Lab helps OTF-supported projects communicate a final product to a wide audience, produce final research write-up reports, copy edit apps and websites, assist with editing, and help OTF-supported projects and fellows as their projects come to a close. Learning Lab vendors include researchers, writers, and designers that report on the successes and lessons-learned of projects.

# Information Controls Fellowship Program (FY2019)

OTF's Information Controls Fellowship Program (ICFP) cultivates research, outputs, and collaboration that examine how governments are restricting the flow of information, cutting internet access, and implementing censorship mechanisms. These efforts help mitigate threats against the ability of global citizens to exercise basic human rights and democracy. Applicants either propose or are connected with a host organization (an entity engaged in the internet freedom space, including academic institutions and civil society organizations). Fellows receive a monthly stipend and small travel budget that varies based on the length of their fellowship.

The ICFP welcomed six fellows in the 2019 application round. The cohort's fellowships concluded in early 2021, completing work on a wide range of projects. Highlights of their accomplishments are available on OTF's website.

## Mohamed Tita

**Host organization:** Stratosphere Research Laboratory at the Czech Technical University

**Duration:** Twelve months

Mohamed researched and documented existing, emerging, and undiscovered censorship circumvention techniques for deployment in Egypt, and worked to minimize burdens for deployment in other repressive environments. The Egyptian government, like others worldwide, has dramatically escalated its censorship tactics in recent years - necessitating the exploration and development of new circumvention techniques. Mohamed worked with the Stratosphere Research Laboratory at the Czech Technical University to carry out their work. An introduction to the project and final outputs can be found on fightcensorship.tech. [27]

## Kris Ruijgrok

**Host organization:** Software Freedom Law Center

**Duration:** Twelve months

Kris documented the social and political circumstances that have led to internet shutdowns, with a focus on India. While India is the world's largest democracy, it also holds the record for having the largest number of internet shutdowns worldwide.

This research explored the underlying legal framework, government motivations behind internet shutdowns, and the role of the private sector. Through in-depth fieldwork in two Indian states where shutdowns are often issued, as well as through analyzing internet shutdown data from the SFLC.in, Kris's project examined the politics behind India's internet shutdowns. While the Indian authorities present the shutdowns as a response to a law and order problem caused by online misinformation, Kris's research emphasizes the shutdowns' political dimensions and shows that they are integral part of the worrying state that India's democracy currently is in. Kris's full paper entitled *Understanding India's Troubling Rise in Internet Shutdowns: A Qualitative and Quantitative Analysis*, was published online.

## Esther Hernandez[28]

**Host organization:** University of New Mexico

**Duration:** Nine months

Esther's research conducted a security and privacy audit of LINE, a popular social media application across Asia. Working with the University of New Mexico, Esther explored LINE's claims that communications on the platform are secure, despite the company not disclosing details of its security and privacy. The research included a technical analysis of the underlying cryptographic protocol for group chat.

[27] https://fightcensorship.tech/blog/2020/09/19/introducing-icarus-project.html

[28] This fellowship concluded early due to unforeseen circumstances.

## Marios Isaakidis

**Host organization:** University of Waterloo

**Duration:** Nine months

Marios assessed the viability of a new circumvention technique that supports low-latency proxying and redundant file storage. Investigating this technique including reviewing incentives-based routing, the effect of BitTorrent "super-nodes", hidden services integration, and exploring their functioning in shutdown scenarios. The technology has the potential to provide a solution to numerous tactics, such as protocol fingerprinting attacks, traffic analysis attacks, establishment of national intranets, bridge enumeration, and the blocking of bridges. A prototype mechanism to address these tactics was released through Biton. A summary of the outcomes of the project was released through OTF's website.

## Phyu Phyu Kyaw

**Host organization:** University of Michigan

**Duration:** Nine months

Phyu Phyu's research investigated information controls in Myanmar prior to the coup in 2021. Myanmar has seen a rapid rise of connectivity in recent years with many unknowns as to how the government is interfering and monitoring online activities. This research identified and analyzed the various surveillance and censorship tactics used by the authorities in Myanmar in an effort to shed light into this otherwise opaque system. In doing so, Phyu Phyu utilized a diverse combination of analytical methods, including technical network measurements, interviews, and research analysis of newspaper archives, media reports, and government publications. The full length report, *The Rise of Online Censorship and Surveillance in Myanmar: A Quantitative Study*, is available on OTF's website.

## Pellaeon Lin

**Host organization:** Citizen Lab, Munk School of Global Affairs, University of Toronto

**Duration:** Nine months

Pellaeon's research conducted a security and privacy audit of TikTok, a short-form video sharing social media application that has become incredibly popular among young internet users. ByteDance, a China-based technology company, developed TikTok, and is the first Chinese-made social media platform that reached global popularity, crossing 2 billion accumulated downloads in April 2020. The technical analysis of the platform looked at the extent to which ByteDance protects user's privacy and security. The full report was released in March 2021, and can be found on Citizen Lab's website.

# Digital Integrity Fellowship Program (FY2019)

OTF's Digital Integrity Fellowship Program (DIFP) sees fellows use their digital security expertise to provide hands-on, comprehensive internal support to organizations and communities most affected by internet freedom violations, such as journalists, human rights defenders, NGOs, activists, and bloggers. DIFP fellows also educate the broader internet freedom community about the threats and vulnerabilities they face, working to ensure that emerging and existing technologies meet the needs of at-risk communities.

The DIFP welcomed six fellows in the 2019 application round. Fellows receive a monthly stipend to aid in completing their fellowships.

## Cristian Leon

**Duration:** Twelve months

Christian's work sought to strengthen capabilities for investigation, documentation, and safeguard of evidence of two human rights organizations in Venezuela and two in Bolivia. The work also provided each organization with digital security assistance to conduct their programmatic activities. This project originated from political crises in each country, as both Venezuela and Bolivia have experienced regressions against most human rights, criminalization of protests, and strong control over information.

## Jorge Sierra Sebastian Guerrero

**Duration:** Twelve months

Jorge's project focused on the protection of digital security and privacy for journalists, investigative reporters, and independent media organizations who are members of the Mexico Border Investigative Reporting Hub (Border Hub). The Border Hub is composed of members reporting on corruption and human rights issues under challenging circumstances in seven border Mexican states, and is considered one of the most dangerous zones for journalists in the world. The project contained three major components, including fostering the digital security capacities of journalists and freelancers, creating a loop of information sharing with the internet freedom developer community, and providing feedback into how border journalists and media organizations are using existing digital security technologies.

## Oriana Marquez

**Duration:** Twelve months

Oriana's fellowship focused on developing the security capabilities of Venezuelan human rights organizations that work in the country's border areas, helping to mitigate the main threats faced by these organizations, which include surveillance by the Venezuelan state, censorship through blocking of websites and social media, ongoing surveillance, and threats of physical harm. The main objectives included raising awareness amongst Venezuelen organizations about the risks involved and the strategies to mitigate them, evading censorship imposed by the Venezuelen state, and improving practices in the management of information and communications of civil society organizations in the Colombian-Venezuelan border.

## Amir Rashidi

**Duration:** Twelve months

Amir's work helped to raise the capacity of Iranian ethnic and religious minority rights organizations to use digital communications in a safe and secure manner. By assessing the security risks and needs of these organizations, the fellow helped to improve security of organizational networks by auditing the security practices of both the organization and its employees, developing tailored information security policy guidelines and training programs, providing digital security training, and providing rapid response support in the wake of security breaches. The work helped those who are in contact with at-risk individuals, such as activists and journalists.

## Tawanda Mugari

**Duration:** Twelve months

Tawanda's fellowship project worked to advance proactive digital security for newly established organizations that support at-risk communities in Zimbabwe. The socio-political context and operational environment for LGBTI communities in Zimbabwe is under threat, despite there being no laws against such groups in the country. By supporting three at-risk LGBTI groups, this fellowship helped to establish the security baseline and threat model for each organization, develop and execute strategic direction for strengthening the digital resilience of each group, sustain secure habits and behaviors for consistent implementation of security controls, and shared learnings from the fellowship with the wider internet freedom community.

## Neil Blazevic

**Duration:** Twelve months

Neil, working with front-line organizations in Uganda, used his fellowship to strengthen their day-to-day resilience and ability to identify and withstand targeted attacks. Civil society in Uganda is often viewed with suspicion by the government as foreign agents or for aligning with opposition movements, leading to civil society groups being under continuous threat due to lack of legal protection and hostile social norms. This fellowship worked with select pro-democracy and LGBTI organizations to develop a mentorship process for digital security training within Uganda's civil society community, strengthened digital resilience, and engaged resources and tools of the internet freedom community to serve Ugandan civil society.

07

# Direct Support with FY2020 Funds

During the period covered by FY2020 funding, OTF funded over 60 innovative projects through the Internet Freedom Fund (IFF) to combat censorship and repressive surveillance, over **20 research fellowships** through both the Information Controls Fellowship Program (ICFP) and Digital Integrity Fellowship Program (DIFP), which support cutting-edge research and digital security interventions, **5 labs** to improve the security, usability, and interoperability of key internet freedom technologies, and **over 15 rapid response interventions** to address digital emergencies.

A full list of all supported projects is included at the end of this report. This section provides an overview of key project highlights from FY2020.

## Technology at Scale (FY2020)

OTF's Technology at Scale Fund supports the large-scale circumvention and secure communication technology needs of USAGM's networks (Voice of America, Radio Free Europe / Radio Liberty, Office of Cuba Broadcasting, Radio Free Asia, and Middle East Broadcasting Networks). The fund solicits technology solutions that help deliver content to audiences in information restricted environments and protects journalists and their sources. The fund also ensures that technologies used at scale by millions of users remain secure and effective.

### NthLink

**$2,950,712**

NthLink is a powerful anti-censorship mobile application capable of circumventing Internet censorship and self-recovering from blocking events. It incorporates strong encryption to protect the information flow between the consumer and the source. Through OTF, NthLink provides circumvention technology services to USAGM.

### Psiphon

**$4,833,708**

Psiphon is one of the most technically advanced and widely used circumvention tools in the world, providing millions of users with uncensored access to USAGM content and the broader internet. Psiphon's technology, which uses a combination of secure communication and obfuscation technologies, has proven consistently effective in the world's most highly censored contexts.

### Lantern

**$1,612,500**

Lantern is a free internet censorship circumvention tool that delivers fast, reliable, and secure access to the open internet. It provides a way to bypass state-sanctioned filtration through a network of trusted users. Through its mobile application, Lantern's peer-to-peer (P2P) functionality allows mobile users in uncensored regions to provide access to content for users in censored regions.

### Lantern Integration in Pangea

**$10,670**

As an extension of Lantern's project with OTF, Lantern's circumvention software development kit (SDK) into Radio Free Europe / Radio Liberty's (RFE/RL) Pangea webapp as an in-app circumvention solution for censored services.

### Tor Secure Access Package

**$404,233**

Tor, short for The Onion Router, is a free and open-source software for enabling anonymous communications. Tor .onion web addresses have proven to be one of the most successful mechanisms in overcoming censorship and protecting those doing so. The "Tor Secure Access Package" involves holistic solutions for each USAGM entity's website and provides an end-to-end solution for USAGM web content to be distributed in censored or surveilled areas.

# Internet Freedom Fund (FY2020)

The Internet Freedom Fund (IFF) is the primary fund through which OTF supports innovative global internet freedom projects. IFF projects are primarily focused on technology development implementation, but also include applied research and digital security projects. OTF continuously solicits IFF project proposals through a fully open, transparent, and competitive process.

## OpenVPN 2.x

### $53,130

OpenVPN is a virtual private network system that is widely used to ensure privacy from surveillance online as well as for censorship circumvention. OpenVPN 2.x aims to improve the performance of OpenVPN servers by offloading the data channel into the kernel space (i.e. operating system), allowing users better performance when adopting OpenVPN, and driving them away from less secure options. All current OpenVPN users benefit from this project, as they use this project's work on their own VPN clients. In addition, the VPN servers they connect to have implemented the changes.

## Deflect Core (Equalit.ie)

### $180,375

eQualitie's Deflect Core project enables freedom of expression and association online for hundreds of civil society, human rights, and independent media websites, enabling their reach to millions of readers from around the world. Deflect Core accomplishes this by protecting these websites from distributed denial-of-service (DDoS) attacks. By sharing their content distribution and attack mitigation technology with the wider community, Deflect Core reduces the prevalence of DDoS as a means of censorship and online repression by raising the cost of such attacks and removing the impunity enjoyed by those organizing the attacks.

## Mapping the Holes in China's Surveillance State

**$60,710**

A vast and growing infrastructure for long-term detention and incarceration has developed in Xinjiang, China over the past decade. However, knowledge about China's network of internment camps is obfuscated by digital censorship. This project proposed to find the location of the entire network of internment camps through a systematic analysis of sites that are censored in Chinese mapping platform Baidu. By comparing the concealed locations in Baidu with those in Google Earth, where blurring or concealment is used to hide a far lower number of sites, it is possible to identify a long list of potential internment camps. The 2020 investigative report from this research uncovered a massive new prison and internment camp system designed to detain and incarcerate hundreds of thousands of Uyghurs, Kazaks, and other Muslim minority groups, and is considered the largest-scale detention system for ethnic and religious minorities since World War II. In 2021, this investigative report won the Pulitzer Prize in International Reporting.

## Multiple Vantage Point Domain Validation

**$150,000**

This project reduced the privacy and security risks for end users on the domain validation protocol. Previously, adversaries on the internet, including repressive regimes, could attack the domain validation protocol, maliciously obtain transport-layer security (TLS) certificates for target websites, and perform man-in-the-middle attacks that bypass protections offered by encryption. This project developed a more secure domain validation protocol known as multiple vantage point domain validation (MVP-DV) to mitigate these attacks.

## No Script Commons

**$125,000**

NoScript Common Library is a collection of reusable modules, APIs, and documentation designed to facilitate the cross-browser development and maintenance of privacy and security browser extensions such as NoScript, HTTPS Everywhere, Privacy Badger, uBlock, and others. The library will help "Mainfest V3 era" class of security and privacy tools survive the restrictions imposed on certain web browsers. The library also aids developers in porting and/or maintaining extensions on mobile browsers.

## Ouinet

**$250,010**

Ouinet is a technology that enables users to circumvent censorship and reduce the effectiveness of network shutdowns, by utilizing peer-to-peer networking and distributed storage to cache content that is requested frequently inside the censored zone. Ouinet is the open source library that powers the Censorship.no (CENO) project, which enables users to access the web and avoid network censorship.

## LAC RPKI Validator

**$75,000**

This project contributed to development efforts surrounding internet routing, which is the process of selecting a path for traffic in a network or between or across multiple networks. Internet routing, while one of the most important components of internet infrastructure, remains unsecure. Routing systems can be easily hijacked to conduct website blocks, eavesdrop on users through snooping, and redirect traffic to bogus destinations. This project responded to these threats by developing a Resource Public Key Infrastructure (RPKI) validator as a method to add signatures that can be used to verify the authenticity of routing information.

### DEfO - Developing ESNI for OpenSSL

### $94,300

DEfo, and its component Tolerant Networks Limited (TN), provides client and server-side support for Encrypted Server Name Indication (ESNI) in OpenSSL. Encryption of SNI values provides a way to circumvent the blocking of specific websites. DEfO also includes the Guardian Project in the process to ensure that OpenSSL with ESNI supports censorship circumvention techniques without requiring any Terms of Service violations in the connection requests. While recent developments in TLS and DNS privacy have rendered significant amounts of metadata about the traffic invisible to network intermediaries, the name of the server is still completely unencrypted information that can be used for pervasive monitoring and censorship.

### Attacking VPNs to Challenge Basic Security Assumptions

### $148,603

Breakpointing Bad investigated fundamental flaws of VPNs and communicated the findings to at-risk populations. The majority of censorship circumvention, privacy, and anonymity tools work in ways that are essentially VPN-like under the hood and are based on tunneling connections through an encrypted tunnel by re-routing locally generated packets on the VPN client device. The project aimed to reveal inherent flaws in VPNs for security and privacy applications and to educate vulnerable populations about the flaws of VPN technology, disclose to necessary parties all vulnerabilities found, and examine potential fixes for VPN issues.

### Digital Democracy

### $193,000

Digital Democracy works to empower marginalized communities in repressive contexts to use technology to defend their rights. Digital Democracy works with human rights and environmental activists to support human rights documentation by providing technical support and building collaborative technology projects. These activists want to be able to map human rights abuses, including photos, testimonies, and geolocations. To fill this gap, Digital Democracy built Mapeo, an open source toolkit designed in partnership with Indigenous communities for collaborative documentation of human rights abuses, with photos linked to geographic information and cryptographic proofs. Mapeo is resilient during censorship, blackout, and with limited or no connectivity, as data can be shared offline between devices. The local-first database does not require any setup and is embedded in the mobile and desktop apps.

### Disguiser: End-to-End Censorship Measurement

### $199,724

Disguiser helps the global internet freedom communities have a better understanding of the new techniques related to information control and censorship and, consequently, inspire new practices and technologies to adapt and provide safe access to communities in repressive environments. Disguiser aims to explore, develop, and deploy a framework that enables end-to-end measurement for accurately and comprehensively investigating global internet censorship practices.

## FOCI Open Access

**$2,800**

FOCI is an annual workshop that brings together academic researchers, activists, and practitioners in the censorship circumvention community. The 11th annual FOCI workshop was hosted through ACM SIGCOMM, with OTF supporting the publication of open access papers. Open access publishing ensures that these published papers are broadly accessible to other censorship circumvention researchers, activists, developers, and practitioners.

## FileZilla

**$60,362**

FileZilla server is a tool that enables people to use secure file transfer protocol (SFTP) to transfer files confidentially. While many ways exist to transfer files online, SFTP remains one of the most private and secure protocols for file transfer, and is still regularly relied upon by many users in countries without a free internet. FileZilla's project with OTF introduced security, privacy, and usability improvements to the FileZilla server software.

## IODA: An Observatory for Realtime Monitoring and Analysis of Internet Blackouts Caused by Censorship

**$253,296**

The Internet Outage Detection and Analysis (IODA) project is a system that monitors the internet, in near-real time, to identify macroscopic internet outages affecting the edge of the network. The IODA tool provides a public dashboard, providing timely information about network outages in near-real-time. It also enables registered users to inspect further and explore data to investigate disruptive events, ensuring our ability to find out about network distributions, providing tool developers with data to analyze the events, and improving abilities to respond to these events.

## Preparing Tor Browser for Android for Mainstream Adoption

**$358,411**

Tor Browser is a widely used circumvention and secure communication solution, and is the only tool of its kind that offers both browser and network level privacy protections. Tor Browser has primarily existed as a desktop-only solution, with mobile solutions being overly slow and cumbersome. However, many of Tor's target users who live under repressive regimes only have access to the internet through their mobile devices. To better cater to their needs, Tor Browser for Android was developed. The goal of this project is to complete a migration of the Tor Browser for Android. This project will also improve performance, usability, and sustainability of the Tor Browser for Android.

## Indigenous Languages Secure Technology Needs Finding

**$164,989**

Through the organization Global Voices, this project maps and documents the language-related challenges facing localization in the adoption and safe use of internet freedom technologies, particularly as it relates to existing networks of front-line digital activists from dozens of communities working in under-resourced languages.

## Internet Freedom Festival

### $504,709

The Internet Freedom Festival (IFF) is one of the biggest gatherings in the world that brings together activists, journalists, developers, humanitarian workers and others working on freedom of expression, privacy and security. 775 participants from 101 countries attended the 2019 IFF. More than 54% of participants are from the Global South and other communities not well represented in the Internet Freedom community. To address the deterioration of community ties and health of internet freedom networks, OTF's support helps the IFF to create and maintain trusted spaces for internet freedom groups to share knowledge and pool resources, ensure at-risk voices are included, and assess and preempt post-COVID challenges.

## Lower the Barrier to Adopt Awala

### $516,684

Awala is a technology that was designed to circumvent complete Internet blackouts caused by repressive regimes. It enables users to communicate with others, even when the Internet is completely down and technologies like VPNs can't be used. Currently there is a lack of apps in the Awala network for the end users. This project aims to make it easier and safer for 3rd party developers to build Awala-compatible apps to circumvent complete Internet blackouts, and run small-scale, controlled pilots with the target audience.

## Mailvelope

### $68,000

Mailvelope is an open source browser plugin that allows users to use OpenPGP standard to encrypt their webmail email services. Mailvelope facilitates email encryption for users of browser based email providers. It comes as a browser extension and allows enhancement of existing web-mailers with functionality to encrypt and decrypt mails. Mailvelope is updating the software to ensure the security of users. This includes improving encryption key discovery, which will make the key server abuse-resistant and simplify the key search, as well as replacing and updating existing modules.

## Mobile Surveillance Monitor

### $285,000

Mobile Surveillance Monitor (MSM) is a multi-source threat intelligence solution designed to analyze and provide insights into active surveillance threats targeting the phones of at-risk individuals and groups around the world. By providing a complete threat intelligence on mobile surveillance, this project increases attention and better understanding of the scale of mobile surveillance. The increased transparency into attacks enables the journalism community, NGOs, and security researchers to improve their forensic capabilities and provide actionable insights needed to compel policy-makers and the industry to improve the security of mobile networks and penalize offenders.

### NoPhish

### $139,625

NoPhish is a web app that builds the skills of internet users vulnerable to surveillance and digital attacks in detecting and defeating phishing attacks. Phishing is a social engineering technique that attempts to acquire sensitive information from an individual. NoPhish aims to be highly accessible and usable, and highly customizable to be effective against phishing attacks on email, social media, and messaging apps.

### OLIP: The Offline Internet Platform

### $55,457

The Offline Internet Platform (OLIP) is a content distribution platform suitable for low, censored or scarce Internet connectivity areas. OLIP is a platform made of 2 complementary layers : OLIP server, a free open source software that allows anyone to turn any computer/device into a local content distribution platform, and the OLIP Marketplace, an online platform that enables users to publish, access, search, browse and download multiple repositories of content. OLIP acts as an “internet buffer” since it allows anyone in a connected area to download pre-packaged content from OLIP marketplace and to serve it to multiple users in areas with Internet censorship or shutdown.

### TibCERT: Rapid RECON Research to Protect Tibetan Cyberspace

### $196,955

The Tibetan Computer Emergency Readiness Team (TibCERT) seeks to create a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community. This project will improve the security of the Tibetan community as a whole but particularly those in Tibet who are most likely to face punishment for their online communication, and those in exile who are at highest risk of targeted online attacks. In order to develop better security measures for Tibetans in Tibet, the project seeks to conduct research to understand how surveillance and censorship work at specific points where Tibetans are targeted, with a focus on the device and app stores vulnerabilities.

### Visualizing and Explaining App Censorship

### $120,000

AppleCensorship.com reveals Apple’s complicity in censorship and surveillance of iOS users by comparing the availability of apps globally. Built upon the existing effort and user feedback, this project seeks to bring greater awareness to this issue by making the apple censorship data easier to search, displaying information in a more accessible way, and working with partner organizations to provide a more complete picture of Apple censorship on a global basis. AppleCensorship.com regularly releases transparency reports that reveal Apple’s complicity in censorship and surveillance of iOS users.

## 5G and Human Rights

## $129,810

The introduction of 5G has had a significant impact on the flow of data streams and the information architecture, altering characteristics of how information is sent, transported, filtered, and routed. 5G infrastructure presents risks that could enable bad-actors to significantly hamper the usage and workings of security protocols related to the new technology. This project analyzes the risks and opportunities of 5G for human rights in general, freedom of expression, and the right to privacy.

## Seaglass IMSI Catcher Detection in Latin America

## $111,088

International mobile subscriber identity (IMSI) is a unique number that identifies each user of a cellular network. IMSI catchers are eavesdropping devices used for intercepting mobile phone traffic and tracking those devices. This project expands studies to detect the use of IMSI-Catchers in a standardized way in Latin America to develop the promotion of the methodology, technical tools, and data obtained. With many activists at risk of having their data monitored, this project can help activists be more vigilant in protecting their data and identities.

## Ricochet / Anonymous Messaging Online Safety (AMOS)

## $30,000

Ricochet is a messenger that provides unobserved, secure, and easy-to-use connection between sources and journalists. The tool is especially useful to journalists who require communications that can defend against a more sophisticated threat model. Ricochet is based on Tor’s onion services protocol (OSP).

## Security Policy Generator

## $100,000

Security policies are crucial in mitigation of the digital security threats faced by civil society organizations every day. However, the time and expertise required to create and implement them can be costly and prohibitive. This project researched security policies with the goal of creating a new, free-to-use online tool for creating custom civil society organizational security policies, ultimately empowering more organizations to improve their digital security capabilities, becoming more resilient to digital attacks.

## Security Training and Support for LGBTIQ Communities and Allies in Indonesia

## $145,190

To better aid LGBT organizations in Indonesia, this project conducts a series of holistic digital security training to assist and work with at-risk organizations. The project comprises basic digital security, refresher courses, advanced training, and mentoring to build crissi management systems and organizational security policies that ensure a sustainable practice of security.

### Certbot

**$182,708**

Certbot, a project through the Electronic Frontier Foundation, aims to close the gap to a fully encrypted web by improving the distribution, usability, security, and sustainability of traffic encryption with HTTPS. Encrypting traffic with TLS is vital to protecting the privacy, security, and even physical safety of Internet users. Browsing the web over unencrypted HTTP has serious problems that make it vulnerable to eavesdropping and content hijacking. HTTPS fixes most of these problems. Certbot has helped millions of website administrators enable HTTPS. Certbot's project widened the availability of free, easy-to-deploy TLS encryption, and improved the stability and sustainability of the client.

### Cooperativa Tierra Comun SC de RL de CV

**$50,000**

Tierra Comun brings together activists, citizens, and scholars who want data to be decolonized, and works with communities in the Global South. Through this project, Tierra Comun will be working with four organizations to ensure that they have the capacity to face the digital risks against human rights defenders and journalists in Mexico. This includes aiding those who face unauthorized communications intervention, lack of digital security protocols, malfunctioning of hardware and software, theft, and loss of information.

### DL-ISAC (equalit.ie)

**$290,805**

As an extension of eQualitie's Deflect project, this project brings the migration tooling of Deflect to a wider audience, improving network defense for civil society organizations, freedom of expression and association with their online audiences. Deflect Labs Information Sharing and Analysis Centers (DL-ISAC) introduces actionable services to share and automate mitigation solutions for web hosts and any individual website platform running its software.

### Dark Crystal

**$161,270**

Dark Crystal is a protocol for distributed data persistence and threshold-based consensus. It has multiple applications in security-oriented tools and it is based on a secure implementation of an algorithm used in cryptography to divide secrets into parts, and dividing them among a group of participants. This project makes sharding technology intuitive and accessible to developers and end-users of existing applications.

### Digital Security Skill Building for Grassroots NGOs in Chiapas

**$61,497**

Grassroots organizations, activists, and independent media are facing increasing surveillance and violence in Chiapas, Mexico. This project seeks to develop a methodology of long-term support processes accompanying digital security training with grassroots organizations in the region, and share the methodology with other digital security trainers.

### Documentation of Cyberattacks, censorship, and other threats in Venezuela

**$144,011**

Venezuela has experienced significant deterioration in internet freedom with an increase in censorship and state-sponsored cyberattacks that have severely limited the human rights of Venezuelan citizens. The need for comprehensive research into cyberattacks and surveillance in conjunction with network measurements became more evident following state-sponsored phishing attacks in 2019, which exposed personal details of tens of thousands of activists. This project expands the documentation, monitoring, and research to include cyberattacks and surveillance to civil society organizations and independent media while strengthening efforts to track and fight against the increasingly sophisticated internet censorship in Venezuela.

### WireGuard

**$250,000**

VPNs are used across the globe as both an access and privacy tool. Unfortunately, most VPNs rely on underlying protocols that have numerous widely known vulnerabilities, massive codebases and significant performance issues. Furthermore, these protocols are increasingly being targeted by repressive governments seeking to prevent users from overcoming censorship. WireGuard was created to address these issues ensuring a lightweight codebase, extensive security review and integration of many important security features lacking in previous protocols such as fail-closed. This project continues to advance these efforts. The WireGuard protocol is fast and secure, built with just 4,000 lines of code, compared to other VPNs which often have over 100,000 lines. This makes it far easier to debug and secure WireGuard compared to standard VPNs. The protocol has been installed in over 10 million Android phones and countless Linux-based systems.

### Geneva - Evolving Censorship Evasion Strategies

**$125,000**

Researchers and censoring regimes have long engaged in a cat-and-mouse game, with censorship evaders finding ways to confuse censors into thinking that traffic is acceptable, and censors patching their system to thwart such efforts. This project takes a drastic departure from the previously manual evade-detect cycle by developing and utilizing techniques to automate the discovery of censorship evasion strategies. The project developed artificial intelligence and trained it against real censors to automatically learn how to circumvent censorship.

### Risk Assessment Workflow for Recommendation Roadmaps (RAWRR)

**$149,102**

For many organizations, organizational security interventions can require heavy data gathering and analysis, reviewing scattered files and building reports from the data. Few organizations and internet freedom projects have a clear picture of their situation, goals, risks, and how each changes over time with the implementation of security measures. This project develops and adopts a standardized organizational security intervention workflow and a software tool built around that workflow.

## IODA

## $291,725

Episodes of politically-motivated interference with Internet access are widespread and frequent. In particular, large-scale connectivity disruptions, even at country-level, are often used by repressive regimes to attack the free flow of information. These events are typically undocumented, unverified, surrounded by uncertainty about their timing, extent, cause, and specific mechanisms of execution. The Internet Outage Detection and Analysis (IODA) platform helps fill this gap. This project is improving IODA's technical capabilities, making the platform more useful and user-friendly, and releasing more timely reports regarding shutdown events.

## Azerbaijan Internet Watch (AIW)

## $87,410

Azerbaijan Internet Watch (AIW) tracks Azerbaijan's internet freedom landscape in real-time. Since its launch in 2019, AIW has published over 70 documented cases of investigations of information controls in Azerbaijan. The project's goal is to offer reliable data for the relevant audience and stakeholders, collect, analyze, and evaluate new developments through various collaborations, and examine how relevant institutions in Azerbaijan restrict information and deploy censorship.

## Organizational Deployment of Secure Distributed Storage with Tahoe-LAFS

## $200,000

Human rights workers see many risks in their daily work. There are multiple levels of sensitivity of information that have to be protected amongst these workers, including protecting stored information on devices, information in transit between communicating parties, protecting information both at rest and in transit on organizational infrastructure, and assuring that services run by the organizations are operational, updated, and secure. This project addresses the threats to the information at rest and shared within the organization by deploying secure file storage and sharing capabilities.

## MaadiX

## $50,800

MaadiX is a project that offers tools, interfaces, and documentation that simplifies the implementation of encryption on servers in an effort to encourage implementation of encryption technologies. The primary goal of MaadiX is to build and deploy an easy and intuitive encryption tool on one's own server without the need for any technical knowledge. New applications and features can easily be added to MaadiX to offer the infrastructures needed by digital and human rights defenders.

## Masaar

## $50,540

Masaar is developing an observatory to document internet censorship in Egypt and collect internet measurements in Egypt, with the aim of analyzing censorship events on websites in Egypt. Masaar will make all measurements available in an open format for individuals and groups interested in internet freedom.

### Measuring and Countering Slowdown as a Censorship Mechanism

### $150,000

While direct blocking is often thought of as a primary mechanism of censorship, slowdowns and throttling of internet connections can be an effective strategy to deter users from accessing censored content. Anecdotal evidence and preliminary research shows that censors are already detecting whether encrypted connections are tunnels that aim to circumvent censorship and slow these connections down intentionally. This project systematically measured slowdown and throttling in China. Additionally, this project built a prototype open source tool that can counteract throttling and investigate ways it can be integrated with existing anti-censorship solutions.

### Improving Lists of Censored Online Content

### $161,518

Test lists of censored content are an important component of measuring internet censorship, as network measurement tools use these lists to determine which websites are blocked. They offer an opportunity to test the accessibility of popular online platforms across multiple countries. However, for many censorship states, the entries on those test lists have seen little updates over the years, which negatively affects the quality of collected measurements. This project updated the lists of 28 countries in Latin America, Asia, Africa, and in the MENA region, and will improve the methodology for maintaining lists of censored online content, involve local organizations in the updating process, and develop a user-friendly intake form that will improve the process of updating the lists. The update provided machine-readable files made up of URLs tested for blocking by network probes. The test lists included a representative sample of popular local websites, organized into 30 thematic categories.

### Secure UX Design Method

### $250,601

The Secure UX Design Method is a methodology and taxonomy designed as a how-to guide for researchers, engineers, product managers, designers, and teams who are working with highly at-risk communities. It is a series of actionable best practices and guidelines for those who build tools for and with marginalized communities from the ideation stage through the finished product.

### Open App Stack II

### $318,499

Open App Stack is a secure and user-friendly platform for Civil Society Organizations and individual organizations to deploy and manage a suite of secure communications, collaborations, and circumvention tools developed by the Internet Freedom community.The project aims at enhancing information security of civil society organizations, and improving the adoption of tools developed by the internet freedom community. Open App Stack also automates the maintenance of these free and open tools. This is particularly beneficial for organizations and individuals who lack the capacities to set up and maintain such systems from scratch. The initial phase of the project has resulted in a prototype of the tool and documentation. The second phase of the project is focused on security testing, usability and deployment among civil society organizations.

### PiGuard

### $72,830

VPNs have been used by activists, bloggers, and journalists for years to secure online communication and circumvent censorship. However, it is quite easy to shut down a service just by blocking the IP address of the server by providing the VPN tunnel service. Utilizing the VPN WireGuard's "IP Roaming" feature, which allows a device to automatically connect to a new VPN server in case the previous server got blocked, PiGuard seeks to embed WireGuard in small and affordable servers to create WiFi hotspots allowing connected users to benefit from an encrypted connection. This project also aims to transfer the technology to independent media and human rights organizations in Africa, MENA, and Eastern Europe.

### Rapid Digital Security Audit for the Egyptian Commission for Rights and Freedoms

### $45,490

Egypt's largest human rights organization, the Egyption Commission for Rights and Freedoms (ECRF) has increasingly experienced a range of digital attacks. These attacks have dramatically increased over the past several years, with the most intense threats following the government's crackdown of the September 20, 2019 protests. This project conducted an urgent and comprehensive digital security audit of the ECRF that entailed a needs assessment and diagnostic of the organizations digital security needs, development of an organizational digital security policy, and implementation of a work plan that incorporates the same.

### Relaynet (later AWALA)

### $127,757

Relaynet (later rebranded AWALA) is a technology that was designed to circumvent complete internet blackouts caused by repressive regimes. It enables users to communicate with others even when the internet is completely down and technologies like VPNs cannot be used. Individuals or organizations transport the data between devices that have no internet connection and devices with access - typically those in a different region. The data is transported using storage devices, WiFi, Bluetooth, and mesh networks. Relaynet utilized OTF support to implement the core of the technology on desktop and Android devices, as well as implementing additional safety features.

### Security Support for Sexual Minority Groups in Nigeria

### $120,000

Nigerian laws enacted in 2014 place incredible risks on the rights and freedoms of LGBTQI people, including harsh prison sentences. The situation puts LGBTQI persons, organizations, and human rights defenders at great risk from both state and non state actors who pose the threat of violence to the community. Organizations on the front line supporting the community collect a lot of personally identifiable information which is currently stored in a number of problematic ways that are subject to loss and discovery. This project provides security training to a network of LGBTQI organizations in Nigeria, building the capacity of human rights defenders to protect them from digital harm.

### Smarter Test Target Selection & Analysis for Global Censorship Monitoring

**$425,880**

Measurement tools are critical to record and ultimately overcome the rapid growth of censorship and surveillance practices that impede free expression and violate civil and human rights. The Open Observatory of Network Interference (OONI) is the leading open source censorship detection platform collecting data from over 200 countries on a monthly basis. This project significantly advanced both the capabilities and proliferation of the platform enabling members of the internet freedom community to rapidly respond to such events in promotion and protection of human rights and democracy. The project improved the monitoring of website censorship, expanded the breadth and granularity of global coverage of censorship events, and empowered community participation in censorship measurement research.

### Tella / Tella Security Upgrade

**$53,300**

Tella is a mobile tool that protects journalists and human rights defenders facing repressive surveillance, including device searches and seizures, interception of and eavesdropping on sensitive communication, and attack against servers. Tella currently allows users to seamlessly hide and encrypt sensitive material in a secure container on their mobile device and secure send this material to the servers of the organization they are working with. This project upgraded Tella security by improving on-device encryption and camouflage to better protect users against physical repressive surveillance.

### MassBrowser

**$91,660**

MassBrowser is a free to use and open source tool designed to circumvent internet censorship. Designed and developed by the Secure Private Internet (SPIN) Research Group at the University of Massachusetts-Amherst, MassBrowser operates with the help of internet users with open access to the internet who volunteer to help censored internet users, instead of relying solely on publicly hosted proxy servers. Volunteers are users residing outside the censored regions who are willing to help censored users gain open access to the internet by allowing them to proxy their traffic through their devices. This project uses OTF support to optimize traffic load, set up and deploy a framework to measure and test performance, and localize and improve the user experience.

### Qualnet

**$248,567**

Qualnet is a multi-platform, secure, anonymous internet independent WiFi communication application for people living in repressive countries. Qualnet has a strong focus on usability and ease-of-use to make communication in situations under censorship and with restricted freedom of speech as easy as possible. This project builds version 2.0 of Qualnet with updated technologies allowing new interconnection possibilities.

### WEPN

## $173,195

WEPN allows people with uncensored internet access to share their access with their affiliates behind censorship using ShadowSocks or OpenVPN protocols. WEPN's open source software runs on affordable off-the-shelf hardware devices that providers can install at their homes and make available for use 24/7. The on-premise WEPN devices use the bandwidth of the owner of the device. This eliminates the expense of dedicated bandwidth and the automatic discovery mechanisms, making it challenging for an oppressive government to discover and block each service. This project streamlines the user experience and reduces centralized dependencies on WEPN servers to enhance privacy and security.

### Zanga

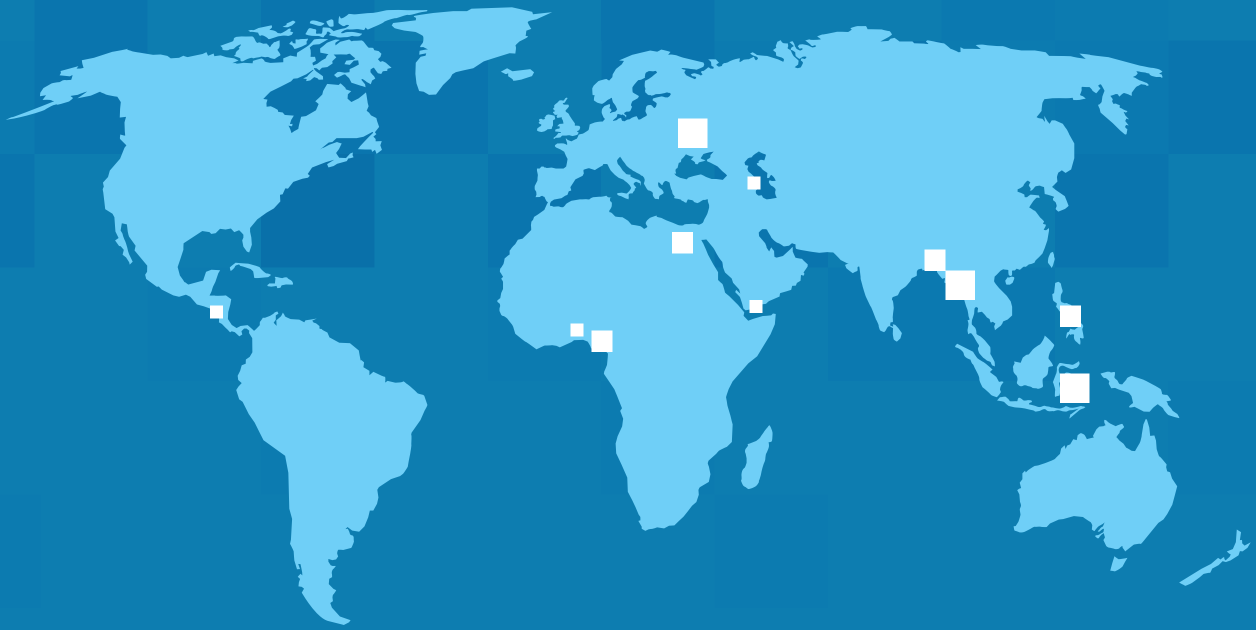
## $95,280

Zanga localizes and adapts Paskoocheh ("alleyway" in Persian) for Arabic users. Paskooche is an open source app store which curates censorship circumvention and secure communications tools. The Arabic platform provides a user-centric, scalable solution for the growing demand in the Middle East and North Africa (MENA) region for access to circumvention tools, and Arabic-language support in investigating, selecting, and using them.

### oLink

## $59,969

oLink is a censorship circumvention tool that does not require any software installation and allows users to access blocked content from a standard web browser. A content provider first mirrors its web pages on a 3rd party platform that the adversary cannot afford to block. The content provider then creates custom URLs that can be distributed via emails, social media, and other means. This project includes high-level system design of the tool, building a content retrieval and reconstruction system, a URL generator, with the outcomes of the project requiring minimal technical knowledge for users to begin using and implementing.



# Rapid Response Fund (FY2020)

OTF's Rapid Response Fund (RFF) provides emergency support to independent media outlets, journalists, and human rights defenders facing digital attacks. The support through this fund helps these individuals and groups stay safe in repressive environments, regain online access, mitigate future attacks, and combat sudden censorship events.

OTF established a network of trusted partners with diverse technical, thematic, and regional expertise to respond to digital emergencies worldwide. The Rapid Response Fund partners expanded their technical service offering and have a greater role in community outreach and communication about the fund services, case identification, referral network triage, as well as management of requests for support.

In FY2020, OTF facilitated timely and comprehensive emergency responses for individuals, communities, and organizations whose free expression had recently been repressed. Within the first month of the Fund's reopening, nine rapid response applications for direct funding were approved. Support through OTF's Rapid Response Fund has provided secure hosting, security audits, and website sanitation to civil society organizations while also providing direct funding for in-country Internet freedom support. For example, OTF's rapid response funds have supported imperiled journalists and civil society groups operating in post-coup Myanmar, where heavy censorship and internet shutdowns have heavily impeded the work of journalists and human rights defenders.

# Labs (FY2020)

OTF provides support to existing internet freedom projects through the organization's Resource Labs (Labs), which aid the internet freedom community in tackling the diverse nature of challenges posed by repressive regimes and authoritarian governments. These resources assist the relatively common needs for tools and technologies operating in this space, and include items such as secure hosting, code audits, communications and localization assistance, usability design, and more. OTF's Labs provide these expert services to the internet freedom community through its five Lab offerings: Engineering Lab, Red Team Lab, Usability Lab, Localization Lab, and Learning Lab. These services ensure that the technologies incubated and supported by OTF are as effective, secure, and usable as possible.

## Engineering Lab

The Engineering Lab focuses on supporting the implementation and inclusion of established technologies into existing applications, organizations, and communities that are advancing internet freedom, supporting the operating and infrastructure costs associated with tool and resource deployment, and conducting assessments of existing apps or websites for recommended privacy, security and anti-censorship improvements. This Lab's service offerings were provided by Greenhost (eclips.is), Throneless Tech, Maxwell Pearl, Combonet, Guardian Project, Mullvad, and Private Internet Access.

### Eclips.is (Greenhost)

**$330,058**

Eclips.is (formerly Greenhost) is a secure cloud resource and a vendor for OTF's Engineering Lab. Eclip.is has emerged as a vital resource for OTF projects and the internet freedom community, helping to manage secure cloud computing infrastructure and web-based platforms for those seeking support through the Engineering Lab. Eclips.is is one of the Engineering Lab's primary service partners.

### Guardian Project

**$346,000**

The Guardian Project aims to create easy-to-use apps, open-source firmware and software libraries, and customized solutions that can be used around the world by any individual looking to protect their communications and personal data from unjust intrusion. Guardian Project became a vital service partner for OTF's Engineering Lab.

### Maxwell Pearl

**$36,000**

As a service provider for the Engineering Lab, Maxwell Pearl provided support for the widespread deployment of internet freedom technology, and support for the platforms relied upon by internet freedom technology. These activities included deployment and support for common anti-censorship and anti-surveillance technologies, reviews of existing technologies to find areas of improvements, and assistance in adoption of such technologies.

### The Public Source

**$5,590**

The Public Source utilized OTF's Engineering Lab to support integration of support tools into their platform. The independent media platform deployed an instance of SecureDrop, a free software platform for secure communication between journalists and sources, to aid in the platform's accountability By integrating SecureDrop, they aim to push for transparency and to free information and data in service of the public interest.

### WebApp

**$334,077**

OTF's Hypha (WebApp) maintains the public-facing website providing informational pages, news, funded project, the team, and advisory council members. More important, the WebApp also manages all aspects of OTF's proposal submission and review workflows. The WebApp's capability to keep up with an ever-growing number of applications and evolving technology best practices directly relates to the OTF team's ability to successfully identify and process the best internet freedom applications. In response to these growing scaling and feature needs along with increased privacy and security considerations, OTF engaged vendors through its Engineering Lab to support the app and meet the team's demands. This includes general software development, new feature development and implementation, software bug fixes, and improvements to safety and security.

## Red Team Lab

The Red Team Lab offers services that look to strengthen the security of open-source internet freedom software by providing security audits, advancing projects' software security best practices, validating privacy and security claims of projects, and more. By focusing on improving the software security of projects that advance OTF's internet freedom goals, supported projects can ensure that the code, data, and people behind each project have the tools they need to create a safer experience for those experiencing repressive information controls online. The work of this lab is primarily reactive by reviewing and responding to issues in pre-existing software, and was supported in FY2020 by the Lab's service partners: Cure53, Include Security, Radically Open Security, NCC Group, and Subgraph Technologies.

### NCC Group Security Services

### $150,000

NCC Group Security Services is a global cyber and software resilience organization operating across multiple sectors, geographies, and technologies. As a Red Team Lab vendor, NCC helps OTF and it's projects by providing detailed professional reports of the findings and recommendations from security audits of programming code and penetration tests of systems. By establishing a high-level of privacy and security standards, NCC conducts independent technology audits, network penetration testing, code audits, recommended solutions for gaps and vulnerabilities, reference materials used to support findings, and more.

### Radically Open Security

### $250,000

Radically Open Security, a non-profit computer security consultancy, aids OTF as a Red Team Lab vendor by providing professional audits of programming code, penetration testing of systems and networks, organizational and operational security training, and providing detailed reports on findings alongside recommended solutions. Radically Open Security's unique non-profit business model supports transparency, openness, and giving back to the community.

### Subgraph Technologies

### $50,000

Subgraph is an open source security company with specialized experience in application security. As a Red Team Lab partner, Subgraph supports the security needs of OTF-supported projects and projects from the broader internet freedom community through security audits and penetration testing based on well-established principles from the security and cryptography industries.

### Cure53

### $250,000

Cure53 offers penetration tests for online services, security analysis and architectural advice, training and consulting, incident management, and web malware analysis. Through the Engineering Lab, Cure53 performs professional audits of programming code, penetration testing of systems and networks, and provides detailed reports of their findings.

### Include Security

### $250,000

Include Security has worked with over 75 clients on more than 200 assessments. Working with a wide range of companies, Include Security specializes in Grey Box security assessments which allow consultants to be significantly more efficient in finding vulnerabilities. Grey Box assessments are conducted where the consultant has access to both a working instance of an application and the source code for the application. Include Security aids OTF and its projects by providing security services for web applications, cryptography services, and adversarial audits.

## Community Lab

The Community Lab provided services that empowered the community to become strong and vibrant by focusing on cultivating deeper trust relationships, improving knowledge share and collaboration, and supporting and diversifying the next generation of leaders. OTF supported the internet freedom community, global and cross-cultural by nature, by helping the community build spaces that empower individuals to network, address existing and emerging needs and opportunities, share resources and knowledge, and collectively strategize.

### Internet Freedom Festival

### $99,620

The Internet Freedom Festival (IFF) is one the largest, most diverse, and most inclusive conferences in the world that brings together activists, journalists, developers, humanitarian workers, and others working on freedom of expression, privacy, and security. In FY 2020, 1000+ activists, journalists, technologists and human rights defenders from over 100 countries gather for a week of sharing and learning.

### Bread&Net / Social Media Exchange (SMEX)

### $64,719

Bread&Net is an Arabic-language conference, organized by SMEX, which brings together stakeholders from across the Middle East and North Africa (MENA) region to strengthen efforts to advance human rights in digitally networked spaces. Bread&Net is a participant-driven gathering, with an agenda that provides space to develop improved strategies for engaging broader, more diverse communities in the development and critique of practices and policies that implicate human rights in digitally networked spaces.

### Localization Lab

**$964,602**

The Localization Lab addresses a major concern of the internet freedom community in tool-localization by helping to cut delays in making internet freedom tools relevant, appropriate, and available for individual countries and cultures. Often limiting the broad adoption of a critical tool, localization supports efforts to provide tools in a given user's native language and expanding the reach of OTF-funded projects. Additionally, prohibitive costs and limited availability of professional translation are some of the biggest hurdles to overcome when deploying Internet freedom tools globally. To address these challenges, OTF's Localization Lab partners utilize a vast community of translators able to provide scalable translation platforms for large or small diverse projects.

### Usability Lab

**$208,699**

The Usability Lab (now the Secure Usability and Accessibility Lab) offers secure usability and user-interface assistance to internet freedom and digital security tools to help them recognize and solve usability challenges that hampered the adoption of those tools in repressive contexts. OTF partners with service providers that offer secure usability and accessibility coaching, consultation, and audits that help the advancement of the internet freedom community and the accumulation of practical knowledge through peer-to-peer learning.

### Learning Lab

**$59,725**

The Learning Lab helps OTF-supported projects communicate a final product to a wide audience, produce final research write-up reports, copy edit apps and websites, assist with editing, and help OTF-supported projects and fellows as their projects come to a close. Learning Lab vendors include researchers, writers, and designers that report on the successes and lessons-learned of projects.

# Information Controls Fellowship Program (FY2020)

OTF's Information Controls Fellowship Program (ICFP) cultivates research, outputs, and collaboration that examine how governments are restricting the flow of information, cutting internet access, and implementing censorship mechanisms. These efforts help mitigate threats against the ability of global citizens to exercise basic human rights and democracy. Applicants either propose or are connected with a host organization (an entity engaged in the internet freedom space, including academic institutions and civil society organizations). Fellows receive a monthly stipend and small travel budget that varies based on the length of their fellowship.

Despite funding being withheld from OTF for much of the year, the ICFP welcomed its seventh fellowship cohort in 2020.This cohort focused on research related to various censorship techniques employed by China and the avenues for circumvention. This includes exploring DNS poisoning through forged IP addresses, interference with popular circumvention protocols, and user-created censorship circumvention techniques on Chinese social media platforms. The ICFP also continued to support research from its sixth class of fellows following delays from both COVID-19 and the pause on OTF programmatic activities.

## Hoàng Nguyên Phong

**Host organization:** Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

**Duration:** Twelve months

Phong previously discovered the prevalence of an abusive DNS poisoning behavior of China's Great Firewall (GFW) in which IP addresses owned by many U.S. companies, including Facebook, Twitter, and SoftLayer, are heavily used in forged DNS responses. A preliminary report for this line of work was presented at USENIX FOCI '20.

During this fellowship, Phong designed a probing method to reverse-engineer the actual blocklist used by the GFW's DNS filter, which led to the creation of GFWatch, a longitudinal measurement platform built to monitor China's censored domains as well as the forged IP addresses being abused. Ultimately, these datasets can assist in the development of effective solutions to bypass and reduce the negative impact of the GFW's DNS filtering on the global Internet. GFWatch is accompanied by a research paper presented at the 30th USENIX Security Symposium in collaboration with researchers from four U.S. and Canadian institutions (Stony Brook University, UMass Amherst, ICSI at UC Berkeley, and the Citizen Lab at University of Toronto).

Using data from GFWatch, Phong also assessed the impact of GFW's DNS censorship on the global DNS system, and proposed strategies to detect poisoned responses that can sanitize polluted DNS records from the cache of public DNS resolvers in order to assist the development of circumvention tools to bypass the GFW's DNS censorship. The full report is available here.

## The Effect of Censorship Circumvention on Information Transmission

**Host Organization:** Not publicly listed

**Duration:** Twelve months

From embedding text in images to rearranging word order of online posts, internet users in China regularly devise creative ways to post content deemed "sensitive" by the government in order to evade censorship. To better understand the most effective  user-generated censorship evasion techniques that maximizes censorship circumvention and information transmission, the fellow used a combination of interviews, experiments, and a nationwide survey in China to test the adoption difficulty, circumvention effectiveness, and informational cost of existing circumvention techniques. The research found that there was generally a trade-off between circumvention effectiveness and information transmission - to be effective in circumventing censorship generally entails altering the original text to a greater extent but doing so can pose a greater challenge for reading comprehension of the altered text. Using specialized tools or language to alter text also increases the adoption difficulty for users.The full report, ***The Effect of Censorship Circumvention on Information Transmission,*** is available here.

## How GFW Detects and Blocks Various Circumvention Services

**Host Organization:** Not publicly listed

**Duration**: Twelve months

The fellow investigated the underlying mechanisms used by China's GFW to identify and block various popular censorship circumvention protocols. There have been many reports from Chinese internet users that their censorship circumvention servers were blocked. At the same time, preliminary experiments suggest that these censorship circumvention servers have been actively probed by the GFW. In the effort to investigate the underlying mechanisms used by China's Great Firewall (GFW) to identify and block various popular censorship circumvention protocols, the fellow demonstrated how the GFW inspected and dynamically blocked any seemingly random traffic in real time. This capability potentially affects many censorship circumvention protocols that use encryption to appear as random traffic, including (but not limited to) VMess+TCP, Obfs4, and many variants of Shadowsocks. The full report, ***Exposing the Great Firewall's Dynamic Blocking of Fully Encrypted Traffic***, is available here. The fellow also built the Great Firewall Report, a platform to monitor internet censorship in China and provide practical guides for users and circumvent tool developers to defend the evolving censorship techniques.

OPEN TECHNOLOGY FUND

2019/2020

**ANNUAL REPORT**