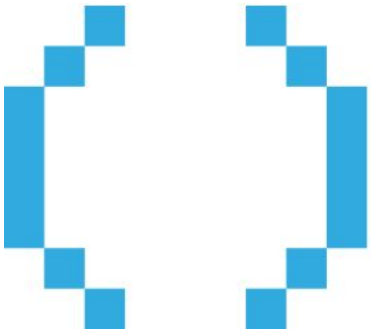


OPEN TECHNOLOGY FUND

# FY 2017 Annual Report

*Open Technology Fund*


The Open Technology Fund (OTF) is a global internet freedom program working to advance the free flow of information online in the world's most closed, repressive places. In an effort to promote open societies and human rights, OTF supports open technologies and communities that increase free expression, circumvent censorship, and obstruct repressive surveillance. A program of Radio Free Asia (RFA), OTF is funded by an annual grant from the U.S. Agency for Global Media (USAGM).

Every project or person that OTF supports is working to achieve a primary outcome that fits within one or more of the following focus areas and objectives:

***Focus Areas:***

- ***Access*** to the internet, including tools to circumvent website blocks, connection blackouts, and widespread censorship;
- ***Awareness*** of access, privacy, or security threats and protective measures, including how-to guides, instructional apps, data collection platforms, and other efforts that increase the efficacy of internet freedom tools;
- ***Privacy*** enhancement, including the ability to be free from repressive observation and the option to be anonymous when accessing the internet;
- ***Security*** from danger or threats when accessing the internet, including encryption tools.

***Objectives:***

- Advance ***research*** about repressive internet interference in modern communication networks and the methodologies and technologies to best circumvent it;
- Foster ***development*** of technologies that circumvent repressive censorship and surveillance or increase communication access and safety; and
- Enable widespread ***implementation*** of solutions in an effort to free people from repressive internet interference.

# Table of Contents

# Executive Summary

Fiscal year 2017 (FY2017)[1] marked the sixth year of funding operations for the Open Technology Fund and its work in advancing the free flow of information online and promoting internet freedom globally in the world's most closed, repressive places. During this time period OTF experienced unprecedented levels of growth in both the number of applications received and the diversity of efforts funded.

OTF has long sought to lower application barriers to global internet freedom funding by conducting bimonthly open calls for concept notes[2]. This process allows the best ideas to advance, no matter where they originate. In FY2017, the number of concept notes submitted to OTF increased from tens per application round to well over one hundred. These concept notes came from every corner of the internet freedom community and every part of the globe. This dramatic expansion in applications increased the competitiveness of OTF funding as well as the quality of the projects and fellows that ultimately received OTF funds. It also revealed encouraging signs that solutions are being informed or designed by the communities experiencing some of the worst instances of internet censorship and surveillance.

Although OTF is best understood when viewed through the specific lenses of the projects, fellows, and labs that it funds, three general themes characterized OTF's overall operations during FY2017: (1) building off previous successes, (2) increasing efficiency and applicant response, and (3) moving closer to the field.

**Building off previous successes**

In 2017, OTF continued to build off the successes it achieved in prior years. The inclusion of the Signal Protocol[3] into Whatsapp, Facebook Messenger, Skype, and other extremely popular communication platforms means that usable day-to-day communications are now more secure than they once were for many around the globe. And the establishment of the Signal Foundation ensures long-term sustainability for Signal, reducing the need for future OTF funding. The Tor Project's anonymity and privacy-enhancing network continues to act as a bedrock internet freedom technology, with numerous internet freedom tools embedding Tor into their products. For example, the Open Observatory of Network Interference (OONI) continued to grow into a

[1] OTF's Fiscal Year funding allotments are not closely aligned with the calendar year. This report covers programmatic spending for OTF's FY2017 funding, which occurred during the latter half of calendar year 2017 and the first three quarters of calendar year 2018.

[2] OTF's primary funding mechanism, The Internet Freedom Fund, employs a two-stage application process in which applicants submit a concise write-up of their proposed project in the form of a concept notes. Applicants whose concept notes are favorably reviewed are then asked to submit a full project proposal before OTF makes a final funding determination.

[3] OTF provided funding to Open Whispers System to support the Signal Protocol from 2013-2016. See OTF's prior annual reports for further details.

mature, vital, and easy-to-use censorship detection tool serving millions of users worldwide and revealing instances of censorship during critical times. Simultaneously, the Tor Browser itself is regularly used by millions of people worldwide. Through our Labs, OTF has supported more than 85 security audits for internet freedom projects, identifying and patching nearly 2,000 vulnerabilities in total, while also enabling the translation of more than 75 tools into more than 200 languages and dialects. OTF has also continued to support events around the world that gather together communities globally, regionally, and locally, further enabling forged connections, partnerships, and awareness raising.

Recent OTF outreach and funding efforts also continue to encourage the development of new circumvention and security technologies that can be built, at scale, into tools that are already operational in the field. These efforts help expand the reach and increase the efficiency of building and deploying new circumvention and security techniques around the world. Additionally, OTF continues to explore new avenues to encourage project sustainability beyond the life of OTF funding by leveraging other sources of government and non-government funds, quasi-commercial models, and in-kind service offerings that can serve as bridges to greater sustainability for internet freedom projects.

**Increasing efficiency and applicant response**

OTF serves those on the frontlines of the fight for internet freedom. Accordingly, it is necessary vbfor OTF to select only the projects it deems most likely to be impactful based on the quality of the solution proposed and the technical and thematic expertise of the applicant. In terms of capacity building, however, it is also important for OTF to provide substantive, constructive feedback to applicants whose projects were *not* selected. This type of feedback allows applicants to develop a better understanding of what is required for a successful OTF submission going forward.

Making funding decisions based on active due diligence, while simultaneously providing detailed feedback to all applicants amidst a sharp increase in the number of concept notes received, has been a significant structural challenge for OTF. Fortunately, investment in an upgraded web-interface application system is helping to improve the efficiency of concept note management, as well as applicant response and program development. As always, OTF is focused on increasing the transparency of OTF operations. Sharing project successes and challenges will better inform future applicants and help ensure learnings are shared more efficiently within the internet freedom field.

**Moving closer to the field**

The best solutions are informed by the contexts in which they will ultimately be deployed. Over the past year, OTF helped to cultivate intra- and inter-regional connections between technologists, human rights activists, researchers, journalists, and others fighting for internet freedom through OTF's Community lab. OTF also worked to make best-in-class solutions accessible to more communities through the work of the Localization and Usability labs. And, for

the first time, OTF hosted its annual summit outside of the United States in an effort to continue to bring OTF's global community closer to important regional internet freedom communities.

In FY2017, despite mounting threats from governments seeking to limit access to information online, OTF, in close coordination with partner programs at USAGM's Office of Internet Freedom (OIF) and the State Department's Bureau of Democracy Human Rights and Labor (DRL), continued to evolve to fulfill its congressional mandate to promote internet freedom globally. And it will continue to do so in the years ahead.

# Internet Freedom Landscape

## Broadened Tactics of Repression

Over the past year, issues pertaining to disinformation, censorship, privacy, and freedom of expression rose to the forefront of societal discourse around the world. Using tactics both new and familiar, authoritarian governments continued to curtail the ability of their citizens to access the open internet, communicate securely, and freely express themselves online. According to Freedom House's *Freedom on the Net* rankings, global internet freedom declined for the seventh consecutive year in 2017, with less than 25% of users in assessed countries living in places where the internet is considered "free."[4] In addition to blocking content and cracking down on the expression of dissenting views, repressive state actors also found ways to exploit the open internet during the period covered by FY2017. These state actions not only cast undue doubt and suspicion on essential democratic institutions like free speech and the free press, they also called into question the very objectivity of "facts" themselves.

Yet despite the emergence of these types of threats and restrictions, the world continued to see rapid growth with regards to internet access writ large, including in categories like connectivity and social media use. In regions where connectivity is expanding quickly, citizens generally welcomed the changes made possible by connecting to the global internet. A 2018 Pew Research study found that in 19 "emerging and developed" countries, rampant growth has continued when it comes to internet use, smartphone ownership, and social media usage.[5] Similarly, a 2017 Pew poll found that a majority of people in six surveyed sub-Saharan African countries felt positively about the role of the internet in their country's development on topics such as education, the

[4] Freedom House, "Freedom on the Net 2017," *Freedom House*, <https://freedomhouse.org/report/freedom-net/freedom-net-2017>.

[5] Between 2015-16 and 2017-18, internet use among the media percentage of adults in 19 surveyed countries grew from 50% to 64%, smartphone ownership from 35% to 42%, and use of online social media sites from 38% to 53%, respectively. See: Jacob Poushter, Caldwell Bishop and Hanyu Chwe, "Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones," *Pew Research Center*, June 19, 2018, <http://www.pewglobal.org/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/>.

economy, and politics.[6] Nonetheless, the promises of opportunity made possible by increased connectivity have also given rise to complex questions. As more and more of the world's population comes online, the primary question is no longer whether connectivity will occur, it is what sort of digital community will exist when it does.

Internet freedom rankings have trended downward for several years, due in part to the variety of different ways in which repressive governments are attempting to control information on the internet to suit their needs. Repressive states no longer simply restrict access to unwanted content. They now try to wield influence over the open internet itself in order to further their agenda. This type of activity includes manipulating freely available online platforms in order to drown out dissenting views, facilitating the spread of state-backed propaganda, and otherwise attempting to control the online conversation. Repressive actors continue to institute online censorship by blocking websites, targeting individuals who express dissenting views by trolling, harassing, and intimidating them (including by levying offline punishments for online speech), filtering out undesirable terms and topics from search results, and sometimes even shutting down the internet outright. Increasingly, censorship has seeped into common digital spaces, which are manipulated and manually engineered to muddy the waters of truth, fact, and popular opinion.

These actions are now all too common. Russia's online efforts—at home and abroad—to implement influence campaigns in an effort to shape the views of netizens have been well-documented.[7] But Russia is not alone. In repressive states like China[8] and Saudi Arabia,[9] online conversations have been flooded with bots and troll armies to "astroturf" certain conversations, slanting political discourse toward state-friendly opinions with an artificial proliferation of pro-government views. In Cambodia[10] and Myanmar,[11] majority, state-backed voices have used popular social platforms like Facebook to spread anti-democratic sentiments and incite violence. And in Iran, the government has sought to create an inclusive, "halal" national intranet, directly contradicting the inherently transnational, cross-cutting nature of the global internet.[12]

---

[6] Laura Silver and Courtney Johnson, "Internet Connectivity Seen as Having Positive Impact on Life in Sub-Saharan Africa," *Pew Research Center*, October 9, 2018, <http://www.pewglobal.org/2018/10/09/internet-connectivity-seen-as-having-positive-impact-on-life-in-sub-saharan-africa/>.

[7] *See, e.g.*, Neil MacFarquhar, "Inside the Russian Troll Factory: Zombies and a Breakneck Pace," *New York Times*, February 18, 2018, <https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html>.

[8] Kemeng Fan, "China's government cracks down on paid internet posts, while employing its own," *Los Angeles Times*, May 12, 2018, <http://www.latimes.com/world/asia/la-fg-china-water-army-20180512-story.html>.

[9] Elias Groll, "The Kingdom's Hackers and Bots," *Foreign Policy*, October 19, 2018, <https://foreignpolicy.com/2018/10/19/the-kingdoms-hackers-and-bots-saudi-dissident-khashoggi/>.

[10] Ben Paviour, "Cambodia Facebook feud hits California courts," *BBC*, February 8, 2018, <https://www.bbc.com/news/world-asia-42828557>.

[11] Paul Mozur, "" https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[12] Jon Gambrell, "'Halal' internet means more control in Iran after unrest," *AP*, January 29, 2018, <https://www.apnews.com/c02a320725fc4afda305a0f3a660dbe6>.

## Blocks and Blackouts

In addition to their attempts to exploit the open internet, authoritarian states also sought to categorically restrict access to certain sites and content during the period covered by FY2017. The governments of Russia and China both moved to restrict use of virtual private networks (VPN), passing laws and introducing rules making use of unsanctioned circumvention tools illegal and subject to fines.[13] After Chinese presidential term limits were abolished in March 2018, China's Great Firewall targeted messages on popular social media platform Weibo containing words like "disagree," "oppose," and "1984."[14] The Chinese government shut down access to 128,000 sites in 2017 alone, as reported by the government's own Xinhua news agency.[15] Beijing also dramatically advanced its invasive, Orwellian surveillance system in the Xinjiang Uyghur Autonomous Region (XUAR), where ethnic minority Uyghur Muslims have been the target of a "re-education" campaign that has resulted in up to one million minority Uyghurs being held in secretive internment camps.[16] With XUAR acting as a testbed for such technologies, China has reportedly moved to export such tools of repression not only elsewhere in China, but also to new markets, including throughout Africa.[17]

---

[13] For Russia, *see*: Ksenia Idrisova, "Explainer: What is Russia's new VPN law all about?," *BBC*, November 1, 2017, < https://www.bbc.com/news/technology-41829726> and Meduza, "Russian lawmakers approve fines against those who circumvent Internet censorship," *Meduza*, June 5, 2018, <https://meduza.io/en/news/2018/06/05/russian-lawmakers-approve-fines-against-those-who-circumvent-internet-censorship>. For China, *see*: AFP, "Foreign companies in China brace for VPN crackdown as March 31 deadline nears," *AFP*, March 30, 2018, <https://www.straitstimes.com/asia/east-asia/foreign-companies-in-china-brace-for-vpn-crackdown-as-march-31-deadline-nears> and James Griffiths, "A software developer just became the latest victim of China's VPN crackdown," *CNN*, October 10, 2018, <https://www.cnn.com/2018/10/10/asia/china-vpn-censorship-intl/index.html>.

[14] Tony Lin, "As China abolishes two-term limit, a siege on digital free speech," *Columbia Journalism Review*, March 16, 2018, < https://www.cjr.org/analysis/china-censorship.php>.

[15] Chris Duckett, "China shuttered 128,000 sites during 2017 internet crackdown," *ZDNet*, January 9, 2018, <https://www.zdnet.com/article/china-shuttered-128000-sites-during-2017-internet-crackdown/>.

[16] David Stanway, "China state paper accuses west of double standards on Xinjiang," *Reuters*, October 18, 2018, <https://www.reuters.com/article/us-china-xinjiang/china-state-paper-accuses-west-of-double-standards-on-xinjiang-idUSKCN1MT00N?il=0>.

[17] Scott N. Romaniuk & Tobias Burgers, "How China's AI Technology Exports Are Seeding Surveillance Societies Globally," *The Diplomat*, October 18, 2018, <https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/>.

Elsewhere, the Egyptian government greatly expanded its list of blocked websites to nearly 500,[18] including the sites of over 100 media organizations.[19] Venezuela honed its online censorship capabilities, preventing censorship circumvention via altered DNS configuration and blocking access to the Tor network and Tor Bridges.[20] Wikipedia, among other sites, continued to be blocked in Turkey, where a new media law passed in March 2018 further expanded the government's ability to control the internet, demanding both foreign and domestic streaming services to register with the country's media watchdog agency.[21] The Erdogan regime now has the legal authority to demand content restrictions. And internet shutdowns continued to proliferate in India and throughout sub-Saharan Africa, with a Global Network Initiative report identifying more than 100 intentional, state-mandated internet disruptions during 2017.[22]

## Policy Trends

### VPN Restrictions

As noted, the governments of Russia and China both recently restricted use of VPNs, passing laws and introducing rules making the use, development, and distribution of unsanctioned circumvention tools illegal and subject to legal punishments including fines and jail time. Russia's law, which went into force in November 2017, does not outlaw the use of VPNs or "anonymizers" outright, but it does dictate that users may not access sites added to a blacklist of banned sites as designated by Roskomnadzor, the country's chief federal censor. Russia's legislative body passed a measure imposing fines on users who break the law to skirt censors. The same law also introduced penalties for search engines that refuse to comply with Roskomnadzor's blacklist by filtering search results in accordance with the blacklist. Google has already come under fire for failing to adhere to the law.[23]

---

[18] Mada Masr, "Neither victory nor defeat: Court refers Mada Masr blocking case for technical review." *Mada Masr*, September 30, 2018, <https://madamasr.com/en/2018/09/30/news/u/neither-victory-nor-defeat-court-refers-mada-masr-blocking-case-for-technical-review/>.

[19] Leonid Evdokimov, Maria Xynou, Mohammad El-Taher, Hassan Al-Azhary, and Sarah Mohsen, "The State of Internet Censorship in Egypt," *Open Observatory of Network Interference (OONI)*, July 2, 2018, <https://ooni.io/post/egypt-internet-censorship/>.

[20] Access Now, "Venezuela blocks access to the Tor network," *Access Now*, June 25, 2018, <https://www.accessnow.org/venezuela-blocks-tor/>.

[21] Paul Benjamin Osterlund, "Turkey marks one year without Wikipedia," *The Verge*, April 30, 2018, <https://www.theverge.com/2018/4/30/17302142/wikipedia-ban-turkey-one-year-anniversary>. The Economist, "Turkey's government takes new powers to censor the internet," *The Economist*, May 24, 2018, <https://www.economist.com/europe/2018/05/24/turkeys-government-takes-new-powers-to-censor-the-internet>.

[22] Jan Rydzak, "Disconnected: A Human Rights-Based Approach to Network Disruptions," *Global Network Initiative (GNI)*, <https://globalnetworkinitiative.org/disconnected-human-rights-network-disruptions/>.

[23] Meduza, "Russia's federal censor wants to fine Google for ignoring its Internet blocklist," *Meduza*, October 25, 2018,

In China, new government regulations dictating how VPNs may be used entered into force on March 31, 2018. Users—including individuals as well as commercial firms—can now only legally use VPNs approved by the government. The new rules build on China's broad-reaching 2017 cybersecurity law and the removal of VPN apps from the Chinese version of Apple's App Store that same year.[24] In October 2018, a Chinese software developer was fined and sentenced to three years in jail for running a website that offered VPN services.[25]

### Cybersecurity Laws

In 2018, the Egyptian government passed a "Cybercrime Law" granting state authorities new ways to justify the surveillance of users and censorship of websites,[26] as well as a "Media Regulation Law" expanding the government's power to regulate and silence critical voices on social media.[27] The Cybercrime law essentially legitimized what the government was already doing in practice, as hundreds of websites had already been blocked. Under the law, the government can block any website that contains illegal material or "poses a threat to national security."[28] The law also establishes harsh penalties for anyone who uses their free speech to express criticism of the government or "values in Egyptian society."[29] Violators of the Cybercrime Law can face fines of over $1 million dollars (USD) and up to five years in prison. The Media Regulation Law, in turn, redefines any social media user with more than 5,000 followers as a member of the media, making such accounts susceptible to the same censorship rules that govern the press in Egypt.[30] In

---

<https://meduza.io/en/news/2018/10/26/russia-s-federal-censor-wants-to-fine-google-for-ignoring-its-internet-blocklist>.

[24] Sherisse Pham, "China's new cyber law just kicked in and nobody's sure how it works," *CNN Business*, June 1, 2017, <https://money.cnn.com/2017/06/01/technology/business/china-cybersecurity-law/index.html>. Rishi Iyengar, "Apple is removing VPN apps that allow users to skirt China's Great Firewall," *CNN Business*, July 20, 2017, <https://money.cnn.com/2017/07/29/technology/china-apple-app-store-vpn-express/index.html>.

[25] Griffiths, "A software developer just became the latest victim of China's VPN crackdown."

[26] Wafa Ben-Hassine, "Egyptian Parliament approves Cybercrime Law legalizing blocking of websites and full surveillance of Egyptians," *Access Now*, June 20, 2018, <https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/>.

[27] Al-Masry Al-Youm, "Parliament approves law regulating press and media," *Egypt Independent*, June 11, 2018, <https://ww.egyptindependent.com/parliament-approves-law-regulating-press-media/>.

[28] Rania al-Abd, "Parliament passes cybercrime law regulating web content and ISP surveillance," *Mada Masr*, June 5, 2018, <https://madamasr.com/en/2018/06/05/news/u/parliament-passes-cybercrime-law-regulating-web-content-and-isp-surveillance/>.

[29] *Ibid*.

[30] Freedom of Thought and Expression Law Firm, "Statement opposing Egypt's legalization of website blocking and communications surveillance," *Freedom of Thought and Expression Law Firm*, September 6, 2018, <https://afteegypt.org/en/statements/2018/09/06/15766-afteegypt.html>.

response, a consortium of more than 40 NGOs from 25 countries called on Egyptian to repeal both laws, calling them "overbroad, disproportionate attempts to give the government full control over cyberspace."[31]

In Vietnam, the National Assembly passed a cybersecurity law in June 2018, introducing new data localization requirements for foreign internet firms while also banning users "from organizing, encouraging or training other people for anti-state purposes."[32] The Vietnamese government is reportedly preparing to enforce the law, which would require companies like Facebook and Google to establish in-country offices and store Vietnamese user data locally inside the country.[33] Amnesty International called the passage of the law "a devastating blow for freedom of expression."[34]

Similarly, China's new Cybersecurity Law requires so-called network operators and social media companies to keep track of users' real names, not distribute banned content, and store data for in-country users locally.[35] The Cybersecurity Law, along with the aforementioned VPN regulations and other similar measures, represent only a portion of the "legal" means being used to justify the Chinese government's increasing crackdown on online speech and media freedom in the country. These laws are often vaguely worded and open to interpretation so that they can be applied in a wide variety of scenarios. This leads to haphazard enforcement, which can make it difficult to predict what exactly will draw the ire of state censors, especially when enforcement varies from one province or city to the next. China's relatively decentralized regime keeps internet users guessing as to what is out of bounds, and what is not, while large-scale content takedowns continue to become more common. In recent months, thousands of websites were removed for "spreading rumors" as part of a campaign against "harmful" content,[36] hundreds of millions of social media posts were taken down for containing "rumors,"[37] and nearly 10,000 social media

---

[31] *Ibid*.
[32] Bao Ha, "Vietnam says cybersecurity law needed to ensure national security," *VnExpress.net*, June 12, 2018, <https://e.vnexpress.net/news/news/vietnam-says-cybersecurity-law-needed-to-ensure-national-security-3762377.html>.
[33] Mai Nguyen, "Exclusive: Vietnam cyber law set for tough enforcement despite Google, Facebook pleas," *Reuters*, October 10, 2018, <https://www.reuters.com/article/us-vietnam-socialmedia-exclusive/exclusive-vietnam-cyber-law-set-for-tough-enforcement-despite-google-facebook-pleas>.
[34] Amnesty International, "Viet Nam: New Cybersecurity law a devastating blow for freedom of expression," *Amnesty International*, June 12, 2018, <https://www.amnesty.org/en/press-releases/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression/>.
[35] Adrian Shahbaz, "Fake news, data collection, and the challenge to democracy," *Freedom House*, <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism#fotn18-section-china-remakes-the-world-in-its-techno-dystopian-image>.
[36] Reuters, "China shuts thousands of websites in clean-up campaign: Xinhua," *Reuters*, September 22, 2018, <https://www.reuters.com/article/us-china-internet/china-shuts-thousands-of-websites-in-clean-up-campaign-xinhua-idUSKCN1M302F>.
[37] Iris Deng, "WeChat has blocked 500 million postings in fight against fake news," *South China Morning Post*, May 7, 2018,

accounts were removed for "spreading politically harmful information" about the ruling Chinese Communist Party.[38] Notably, similar legislative measures have been proposed elsewhere, including in Thailand,[39] Ukraine,[40] and Honduras.[41]

### Social Media Taxes

A trend emerging across sub-Saharan Africa is the introduction of social media taxes that charge users to access popular apps, websites, and voice-calling services. Since July 1, 2018, Ugandans have been required to pay a fee of 200 Ugandan shillings ($0.05 USD) per day to access and use a list of 58 popular sites, including Facebook, WhatsApp, Twitter, and Skype.[42] Following in Uganda's footsteps, Zambia and Benin recently introduced their own taxes, justifying the move through economic terms at the expense of users and the associated negative impact on freedom of expression.[43] In Tanzania, the government introduced new regulations requiring all media outlets, including of individual bloggers, to pay registration and licensing fees that add up to more than two million Tanzanian shillings (roughly $920 USD) per year.[44] Such regulations make it effectively impossible for individual content creators to freely express themselves through written or video blogs.

## Censorship and Non-State Actors

Although state actors are usually the most culpable actors when it comes to directing online censorship, they do not always implement the actual censoring themselves. Censorship takes place through a variety of different means across various levels of the internet architecture, from

---

<https://www.scmp.com/tech/china-tech/article/2144900/wechat-has-blocked-500-million-postings-fight-against-fake-news>.

[38] Reuters, "China scours social media, erases thousands of accounts," *Reuters*, November 12, 2018, <https://www.reuters.com/article/us-china-censorship/china-scours-social-media-erases-thousands-of-accounts-idUSKCN1NI0BR>.

[39] Patpicha Tanakasempipat, "Thailand plans cyber network scrutiny, law to toughen online monitoring," *Reuters*, June 19, 2017, <https://www.reuters.com/article/us-thailand-cyber/thailand-plans-cyber-network-scrutiny-law-to-toughen-online-monitoring-idUSKBN19A12P>.

[40] Interfax-Ukraine, "SBU supports bill that helps temporarily block websites," *Kyiv Post*, July 6, 2018, <https://www.kyivpost.com/ukraine-politics/sbu-supports-bill-that-helps-temporarily-block-websites.html>.

[41] Human Rights Watch, "Honduras: Cybersecurity Bill Threatens Free Speech," *Human Rights Watch*, April 9, 2018, < https://www.hrw.org/news/2018/04/09/honduras-cybersecurity-bill-threatens-free-speech>.

[42] Lydia Namubiru, "How Uganda is implementing its controversial social media tax," *Quartz*, July 3, 2018, <https://qz.com/africa/1319826/how-ugandas-social-media-tax-works-with-whatsapp-facebook-twitter-blocked/>.

[43] Reporters Without Borders (RSF), "After Uganda, Benin and Zambia impose "worrying" tax on social networks," *Reporters Without Borders (RSF)*, September 21, 2018, <https://rsf.org/en/news/after-uganda-benin-and-zambia-impose-worrying-tax-social-networks>.

[44] John Aglionby and David Pilling, "Tanzania's bloggers face hefty fees for right to post online," *Financial Times*, April 22, 2018, <https://www.ft.com/content/36098722-4623-11e8-8ae9-4b5ddcca99b3>.

internet service provider to Domain Name System (DNS) to Deep Packet Inspection. The internet's development is shaped by both state and non-state actors from the government, the private sector, and civil society. For example, over the past year private companies like Amazon and Google decided to end the ability of their cloud customers to use "domain fronting" to avoid censors in places like Egypt and the United Arab Emirates[45] or when using tools like Signal and Telegram.[46] Similarly, Apple moved to comply with local laws in China by storing Chinese users' iCloud data on the servers of in-country partner Guizhou-Cloud Big Data, raising human rights concerns around how and when Chinese authorities would be able to access user data.[47] And Google is reportedly developing a censor-friendly search engine dubbed "Dragonfly" custom-made for the Chinese market, with terms such as "human rights," "student protest," and "Nobel Prize" blacklisted.[48] More generally, various inherently insecure aspects of the internet continue to present challenges to users in closed societies, such as privacy concerns around the lack of encrypted DNS traffic persisting.[49] Against this technological backdrop, at-risk users from human rights, press, and civil society groups continue to face advanced attacks from state level adversaries, often with the aid of expensive, sophisticated spyware.[50]

## Enabling Dialogue, Demanding Freedom

Despite these challenges, there is ample evidence that the global, open internet remains a powerful tool for enabling freedom of expression and spreading awareness of fundamental human rights for those living in repressed societies. The feminist-powered #MeToo movement made headlines not only in the West, but in China as well, where women from across Chinese society were empowered to speak out on platforms like WeChat and Weibo against long-standing

---

[45] Moxie Marlinspike, "A letter from Amazon," *Signal*, May 1, 2018, <https://signal.org/blog/looking-back-on-the-front/>.
[46] Stephanie Whited, "Domain Fronting Is Critical to the Open Web," *Tor Project*, May 4, 2018, <https://blog.torproject.org/domain-fronting-critical-open-web>.
[47] Nick Statt, "Apple's iCloud partner in China will store user data on servers of state-run telecom," *The Verge*, July 18, 2018, <https://www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security>.
[48] Ryan Gallagher, "Private Meeting Contradicts Google's Official Story on China," *The Intercept*, October 9, 2018, <https://theintercept.com/2018/10/09/google-china-censored-search-engine/>.
[49] *See*, *e.g.*, Thomas Claburn, "How's that encryption coming, buddy? DNS requests routinely spied on, boffins claim," *The Register*, August 20, 2018, < https://www.theregister.co.uk/2018/08/20/dns_interception/>.
[50] *See*, *e.g.*, Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, "Hide And Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *Citizen Lab*, September 18, 2018, <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, Scott-Railton, and Deibert, "Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces," *Citizen Lab*, August 8, 2018, <https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces/>; and Marczak, Alexander, McKune, Scott-Railton, and Deibert, "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," *Citizen Lab*, December 6, 2017, <https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/>.

injustices.[51] Such platforms are subject to heavy-handed state censorship, but the movement flourished nonetheless—thanks in part to the ingenuity of Chinese netizens familiar with inventing linguistic alternatives to avoid censors.[52] In Russia, citizens took to the streets to protest the government's decision to block access to the popular messaging app, Telegram,[53] which saw a Streisand-effect surge in user traffic amidst the attempted block.[54] Notably, while attempting to block the app the Russian government blocked upwards of 16 million IP addresses owned by cloud providers Amazon and Google, marking the first known instance in which a state took such a radical, en masse blocking approach.[55] And in Iran, the use of circumvention tools skyrocketed after the government ramped up its blocking of Telegram and other popular social media tools amidst nationwide anti-government protests, allowing proficient citizens to resist the Iranian regime's attempt to cut off the flow of information during a crucial time.[56]

[51] Han Zhang, "One Year of #MeToo: How the Movement Eludes Government Surveillance in China," *The New Yorker*, October 10, 2018, <https://www.newyorker.com/news/news-desk/one-year-of-metoo-how-the-movement-eludes-government-surveillance-in-china>.
[52] China Digital Times, "Grass-Mud Horse Lexicon," *China Digital Times*, <https://chinadigitaltimes.net/space/Main_Page>.
[53] BBC, "Russia internet freedom: Mass rally in Moscow against Telegram ban," *BBC*, April 30, 2018, <https://www.bbc.com/news/world-europe-43948618>.
[54] Meduza, "Four days of blocking Telegram in Russia and here we are," *Meduza*, April 19, 2018, <https://meduza.io/en/feature/2018/04/19/four-days-of-blocking-telegram-in-russia-and-here-we-are>.
[55] Vlad Savov, "Russia's Telegram ban is a big, convoluted mess," *The Verge*, April 17, 2018, <https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban>.
[56] Alexander J Martin, "Iranian web crackdown drives surge in privacy technology," *Sky News*, January 1, 2018, <https://uk.news.yahoo.com/iranian-crackdown-drives-surge-privacy-technology-193200739.html>.

# Direct Support with FY2017 Funds

OTF provides critical funding and service offerings to projects and individuals pursuant to its core mission of increasing unrestricted access to the internet. While OTF strives to innovate as a funder, the program itself is ultimately defined by the projects, fellows, and labs its funding and service offerings help make possible. Detailed below are the efforts funded by OTF's FY2017 allotment.

## Internet Freedom Fund

### CiviCDR

**$90,000**

Focusing primarily on Iranian civil society, the CiviCDR project platform strengthens the digital resilience of regional journalist and activist communities by creating a platform to efficiently coordinate incident response and facilitate information sharing about collective threats and appropriate responses.

### DNS Privacy

**$306,000**

The DNS Privacy project improves the adoption of encrypted Domain Name Service technologies by providing data on the operational realities of protocols such as DNS-over-TLS, documenting best practices, and encouraging mainstream Domain Name service providers to offer open DNS privacy services to the general public for free.

### STARTTLS Everywhere

**$200,000**

STARTTLS is a solution to address a longstanding vulnerability affecting all email exchanges. The development and implementation of Transport Layered Security (TLS) encryption helps address

the issue, but even when TLS encryption is used, it lacks a mechanism to ensure emails are delivered securely, and it can also be easily disabled by repressive actors. To assist in STARTTLS proliferation, STARTTLS Everywhere provides an MTA plugin for the Certbot tool to help users properly set up their TLS configuration. The project also establishes a submission website, as well as a configuration and management workflow for STARTTLS Policy Lists.

### NoScript (CrossBrowser)
### $100,000
NoScript is a popular privacy and security enhancing browser extension for Mozilla Firefox. "Cross-Browser NoScript" leverages the new Chromium-compatible WebExtensions API provided by Mozilla, and the closely related standardization effort in the W3C Browser Extensions Community Group, in order to make NoScript also support the other major modern browsers (such as Google Chrome).

### GlobaLeaks
### $109,167
The GlobaLeaks project focuses on taking GlobaLeaks from a successful prototype to a mature and stable "product-level" software by adding components targeting long-term support and improved stability, simplifying HTTPS integration, providing ready-made configuration sets for the common whistleblowing scenarios, and easing the deployment of the software by NGOs and providers.

### WeChatScope
### $122,000
The WeChatScope project is a system designed to collect, analyze, and visualize censored messages for public accounts on Wechat, China's dominant social media platform. The data and analyses from the project are being publicly published and shared with researchers and activists working on exposing censorship practices on the Wechat platform via an API. Work is underway to develop a data visualization website and engage community studies on WeChatScope data.

### OONI
### $300,000
The Open Observatory of Network Interference (OONI) is the leading open source censorship detection platform continuously collecting data from thousands of networks across more than 200 countries. Measurement tools like OONI are critical to record, and ultimately overcome, the rapid growth of censorship and surveillance practices impeding free expression and violating rights. OTF's OONI support creates a Windows and MacOS standalone desktop client. It also improves the tests included in the platform around network outages, and further engages on the ground communities in deploying probes, analyzing data, and publishing results. These outputs

better enable members of the internet freedom community to rapidly respond to events in promotion and protection of human rights and democracy.

### Tor Node Distribution Latam

**$89,700**

The Tor Node Distribution Latam project seeks to set up more Tor network nodes in Latin American and grow the Tor user base in order to make the Tor network stronger and safer. This is important to do because even though many internet users in Latin America currently rely on the Tor network to guarantee their privacy and to circumvent censorship online, most of the Tor network nodes are in the Global North. The Tor Node Distribution LatAm project will also help build a stronger technical community of people working around privacy and anonymity in Latin America. The project consists of four phases: set up Tor exit nodes in the region, create materials in Spanish, raise general awareness, and trainings/workshops.

### Suspicious Email Submitter

**$55,000**

The Suspicious Email Submitter, built by Lilia Markham, is an extension for common web browsers that enables the user in one-click to submit a suspicious email with all the necessary information to a pre-configured destination for further analysis. This extension will help combat the malware delivery and phishing emails that have become an increasingly sophisticated and recurring threat. The Suspicious Email Submitter will be easily configurable for use by other organizations and communities both within, and beyond, the internet freedom space. The extension will help rapid responders and other digital security researchers to receive and evaluate suspicious emails sent to civil society, activists, and other people who may be targeted for their activities online.

### IUCRC Research

**$50,000**

As part of the IUCRC mechanism, the University of South Alabama carried out two research tasks focusing on the use of digital forensic techniques to determine: 1) the amount and type of data retained after a hard wipe on a phone that could be used by an attacker, and 2) the detectability of digital attacks through hardware device measurements. This project is particularly notable for the amount of funds leveraged through the IUCRC mechanism. Including funds from NSF and private industry partners, OTF's $50,000 investment is leveraged with more than a half million dollars in additional funding.

### Tor Usability

**$16,250**

The Tor Usability project improves the usability of the Tor Browser Bundle. In general, Tor technologies provide a critical safety tool for those targeted by repressive government actors. Because of its singular benefits, the Tor network and browser are used by more 1.5 million people

each day including journalists, activists, political dissidents, human rights workers, whistleblowers, companies, and privacy-sensitive individuals worldwide. However, research and feedback from existing users, activists, and people who teach Tor indicates that Tor can be difficult to use—but small usability adjustments could alleviate these challenges. Tor's privacy and security features are unparalleled, but if users struggle to obtain, install, and use the software, it doesn't matter how good Tor is. Accordingly, OTF funding supported a designer to work with Tor's development team in designing and adding new features to address those parts of Tor that are unclear or difficult to use. The majority of these efforts can be seen in the 8.0 release.

### Ionosphere
**$30,000**

Ionosphere mitigates the risk of communicating via group messages by building on the Hubot bot platform and the Signal secure communication application to create a bot that sends messages to a group of people, but preserves their privacy by ensuring that the list of phone numbers is not visible to all members of the group. This type of risk mitigation is important because many activists, journalists, and others depend on group messages in order to communicate and spread information. In repressive contexts, however, it is often not desirable to expose the people on a list to each member of the group, as doing so may put the members at risk.

### Briar
**$116,400**

Briar is an open source messaging app designed for activists, journalists, and anyone else who needs a safe, easy, and robust way to communicate. Users can create blogs, forums, and private discussion groups without depending on centralized service providers. Briar is able to function with or without internet access. The project is currently focused on making the app more competitive in its features and performance. Beta testing of over 30,000 users has shown the app is stable and easy to use, but power consumption is too high. The project is working to improve battery life and implement the features most often requested by users: image attachments, adding contacts remotely, improvements to the sign-in process, and a dark UI theme for nighttime use. The project is also developing a headless version of the app that can run on a server or desktop, enabling organizations to integrate Briar blogs and messages into their communication workflows. Support for Tor bridges is being added to strengthen Briar's connectivity in countries where Tor is blocked and to establish a reproducible build process so users can be sure the app they are using is from the published source code.

### Tor Bug Bounty
**$20,000**

The Tor Bug Bounty project supports the ability of researchers to discover and responsibly report bugs in critical Tor infrastructure. This helps Tor ensure that the platform remains secure and anonymous. The Tor Project is only offering bug bounties for two of its core products, Tor (the

network daemon) and Tor Browser. Both Tor and Tor Browser bounties come with different tiers accompanied by a price range and some restrictions.

### NewNode
**$150,000**

The NewNode project is creating a software development kit (SDK) for content delivery through secure peer-to-peer distribution that works even if access to the source of the material is blocked. The utilization of peer-to-peer technology provides a means to bypass filtering and deep packet inspection technology deployed on national gateways and internet service provider networks. NewNode allows any app incorporating it to provide access to content faster, cheaper, more reliably, and in a censorship-resistant manner. When a publisher uses the SDK, users in restrictive countries can access their content without any negative performance impact—even if the publisher is censored in their country—by getting it from a peer. OTF's funding supported the first of two phases for the project. In the first phase, NewNode developed a specification for the transport encryption and the peer protocol while engaging with a small number of beta testing partners. The second phase will further improve the underlying technical components and formally release the SDK.

### OpenArchive
**$245,392**

OpenArchive is a free, open-source mobile application that securely uploads media created on mobile phones to collections stored in a public trust. This helps ensure that journalists, activists, and citizens in repressive countries are able to preserve media they have collected in an application that is safe from censorship or deletion by state or non-state actors. OpenArchive provides a unified user experience that combines several key internet freedom projects, including Creative Commons, the Internet Archive, Tor, and Guardian Project.

### Africa Cyber Threat Modeling
**$57,200**

The Africa Cyber Threat Modeling project detects, documents, and analyzes current and emerging cyber threats with a long term goal of mitigating their impact on users at risk in specific Sub-Saharan African countries, especially around elections. The project studies Togo, Nigeria, Cameroon, Zimbabwe, and South Sudan. Through a combination of technical and investigative means, the project examines models of cyber attacks, including the tools employed for attacks, appropriated strategies or tactics (such as blocking of website pages), phishing, and other social engineering methods.

### OpenAppStack (phase 1)
**$267,991**

The OpenAppStack (phase 1) project seeks to build 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 works to enhance information security of civil society organizations and improve the adoption of tools developed by the internet freedom community. OpenAppStack automates the maintenance of free and open tools, which is particularly beneficial for organizations and individuals who lack the capacities to create and maintain these systems themselves.

### Tibetan Computer Emergency Readiness Team (TibCERT)

**$244,050**

The Tibetan Computer Emergency Readiness Team (TibCERT) project is working to create a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community, as well as expanding Tibetans' technical research capacity on threats in the diaspora and surveillance and censorship in Tibet. The project's goal is to help ensure greater online freedom and security for Tibetan society as a whole. This is important because Tibetans, both within organizations and individually, currently have inadequate resources to defend themselves from online threats, which include the most highly sophisticated actors in the world; the Chinese government regularly targets Tibetan groups and effectively uses Tibet as a "testing ground" in developing new targeting tools and techniques. There is no formalized communication system or process for sharing information between different stakeholders, initiating research projects, or responding to attacks. There is therefore a need to create a permanent platform enabling Tibetan organizations to share, analyze, and develop real-time responses to threats. The platform being created by the project is also helping facilitate engagement between researchers and the Tibetan community to analyze the particular threats Tibetans face, and create potential solutions.

### ServerSide Blocking

**$250,000**

The ServerSide Blocking project investigates an oft-ignored aspect of censorship research: the role of private sector actors such as VPN providers, content delivery networks (CDNs) and other server operators play in carrying out state-mandated censorship. This server-side blocking occurs when these actors prevent content they host from being accessed by users in certain remote locations. The project measures a key form of internet balkanization, and offers best practices for accounting for the phenomenon in studies of country-level censorship. Internet balkanization is an emerging threat to global connectivity, yet currently little research has been done in this area—making it difficult to track and understand the extent of the phenomena. Accordingly, the ServerSide Blocking project is building on its previous work to: (1) develop scientifically rigorous measurement methods to detect server-side blocking, (2) build a system to continuously and globally collect data on the phenomenon, (3) curate tools for mapping and comparative analyses of the data, and (4) provide the raw data and relevant analysis in a centralized and easily accessible repository.

### CGIProxy Improvements

**$69,900**

The CGIProxy Improvements project is working to improve CGIProxy, a tool that allows users to bypass censorship to view and share web content in repressive environments. CGIProxy is currently available in 15 different languages and is considered to be one of the most used tools of its kind in China. It is particularly useful for oppressed populations because it is clientless, can be used on mobile phones, and provides a solution for challenges that vulnerable users face in internet cafes when they are unable to install client-side software. The CGIProxy Improvements project is enhancing the tool by: (1) adding automatic upgrades, (2) improving the user interface; and (3) documenting and measuring unique users and traffic. These improvements will help ensure that users have access to the most secure and efficient version of the software, while also improving ease of use.

### Digital Security Support in Pakistan

**$62,969**

The Digital Security Support in Pakistan project is working to expand the operations of the Digital Rights Foundation's cyber harassment helpline and enhance its digital security capacity to provide support to human rights defenders and activists online. The project specifically increases the numbers of hours and personnel available at the helpline—something that is necessary given the huge influx of demand (1,476 calls in the helpline's first year alone). This type of support is important because digital spaces are increasingly coming under attack in Pakistan, with enforced disappearances, cyber harassment, and stringent free speech regulation in the form of the Prevention of Electronic Crimes Act 2016. These trends are serious impediments to digital freedoms and the work performed by the Digital Rights Foundation. In Pakistan, many activists are targeted specifically on the basis of their speech in online spaces. Because a significant portion of callers to the cyber harassment helpline face problems concerning hacked devices and accounts, a dedicated digital security expert for the helpline is being added as well. This expert will dispense advice on how to guard against fake profiles, blackmailing, and information leaks.

### Securing MENA Publishing

**$48,927**

The Securing MENA Publishing project conducts research in Egypt, Syria, and Jordan—three countries where independent digital media publishers are facing an unprecedented crackdown and heightened censorship. The project investigates these concerns and proposes practical solutions for organizations to produce content securely, including hosting, communication, and producing/publishing. It also helps audiences in the Arab World, where publishing and accessing digital content can be difficult or dangerous, to access content freely and securely through VPNs, mirror sites, and other methods.

### OONI Dashboard

**$33,240**

The OONI Dashboard project improves accessibility for the OONI project, which collects and makes available detailed data on internet interference. The OONI project's current dashboard is not easily usable for the needs of civil society organizations, journalists, researchers, or the general public. The OONI Dashboard project addresses the immediate need for easy to read dashboards so more users can make use of censorship measurements to support their work and increase public awareness of internet censorship. The project makes use of OONI's public API to develop an online dashboard for several countries in South-East Asia, that will provide users with a simple dashboard to quickly see the state of online censorship for their respective countries against categories such as freedom of expression and media freedom. OONI's efforts are important because the state of online censorship for different categories, such as freedom of expression, is currently only reported through manually compiled annual country reports. These reports are a collection of news reports, often with anecdotal and non-technical confirmation of censorship.

### Magma

**$50,000**

The Magma project provides a research framework to people working on information controls and network measurements, particularly in authoritarian contexts and high-risk areas. The Magma guide will enable these individuals to properly structure an activity plan, make informed choices regarding the required tools (including ethical and security aspects), and analyze the data produced by such tools. The project also explores additional improvements that could be implemented in existing network tools to increase their effectiveness in light of measurement needs. The final project outputs will be a comprehensive set of resources to guide those seeking to carry out targeted censorship testing using the OONI-Probe platform and accurately analyze the results. This will make carrying out projects of this nature more accessible and accurate.

## Core Infrastructure Fund

For internet freedom tools to be effective and secure, the basic foundations upon which the are built must also be functional and secure. Beginning in 2015, OTF recognized that a number of the core infrastructure technologies relied upon by internet freedom tools were not sufficiently supported, which in turn limited and constrained the development of internet freedom tools. The technologies that constitute core building blocks of everyday internet freedom tools require alternate criteria for evaluation and support; traditional metrics often fail to capture the effectiveness of these technologies and their integral role in the internet freedom technology ecosystem. The target user for a Core Infrastructure Fund project is often not an end-user, but rather a *developer* of end-user tools. Every year, OTF sees more technologies moving into this realm, and receives more applications for their support. In turn, the amount of core infrastructure

projects OTF supported in FY2017 increased markedly over previous years, to over $400,000. While OTF remains committed to supporting vital core infrastructures, OTF's broader hope is that the success of these core infrastructure projects will instigate commercial companies who have benefited from many of these fundamental technologies to invest in the maintenance, evolution, and security of core internet infrastructure as a vital public good.

### HTTPS Everywhere Else

**$21,00**

Unencrypted HTTP requests leave users vulnerable to surveillance, content filtering, and, in some cases, content tampering. Although the number of websites accepting encrypted connections available is steadily increasing, only a fraction of websites redirect visitors to their HTTPS version by default. HTTPS Everywhere Else provides a way to automate client-local TLS upgrades as a privacy enhancing measure to complement efforts to encourage broader and safer adoption of HTTPS-as-default.

### Securing Domain Validation

**$300,000**

The Securing Domain Validation project is facilitating a deeper understanding of the attack surface of the domain validation protocol to inter-domain routing attacks, as well as the development, deployment, and refinement of secure countermeasures. This is important because adversaries on the internet, including repressive regimes, can currently attack the domain validation protocol, maliciously obtain TLS certificates for target websites, and perform man-in the-middle attacks that bypass protections offered by encryption.[57] Previous research carried out by the project's applicant demonstrated the ease with which a repressive government can exploit these vulnerabilities to harm at-risk communities.

### Tor Metrics

**$73,700**

Tor Metrics is the central mechanism for providing publicly accessible information on a wide range of data points. This transparency is unique to The Tor Project among access and privacy tools, and allows anyone to evaluate the functionality and ongoing relevance of these access and security technologies to the internet freedom community. This project improves the quality, volume, and transparency of the metrics system through the creation of a technical white paper describing the entire measurement and metrics production process, as well as a specification for statistical assessment of aggregate data. The nature of this documentation serves to further encourage other internet freedom tools to follow suit.

[57] For more on the inherent insecurity of internet routing, see: Yixin Sun, Annie Edmundson, Henry Birge-Lee, Jennifer Rexford, and Prateek Mittal, "Routing Attacks on Internet Services," *Freedom to Tinker*, April 11, 2018, <https://freedom-to-tinker.com/2018/04/11/routing-attacks-on-internet-services/>.

### BIND9 Qname Minimization

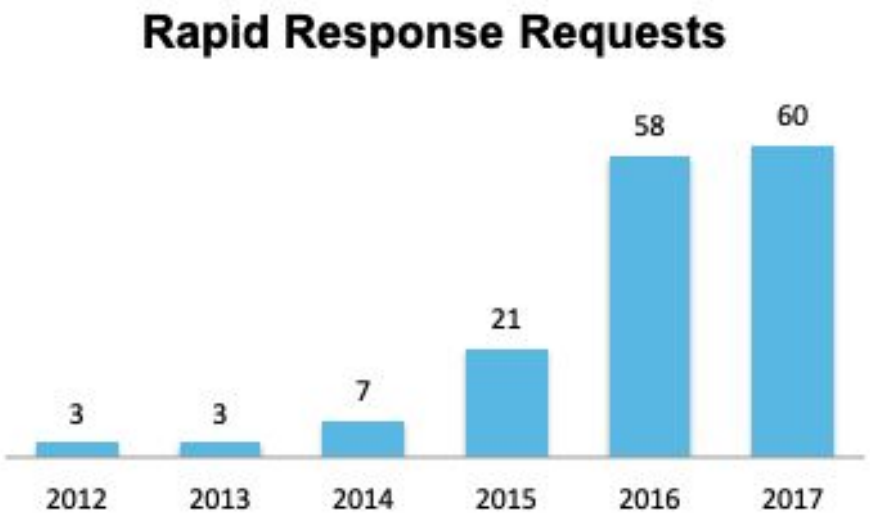
**$78,636**

The BIND9 Qname Minimization project provides enhanced overall privacy to users on the internet by preventing data leakage. Every website must use DNS in order for users to find them easily, but repressive governments are now storing and analyzing these "lookups" in order to surveil users. This project, therefore, works to minimize meta data leakage that could expose email conversations, websites visited, or other potentially sensitive information.

## Rapid Response Fund

The Rapid Response Fund is a broad initiative facilitating the development of a strong digital emergency response community that is able to work together to resolve threats in a timely and comprehensive manner. OTF offers a permanently open application window to ensure it is able to act quickly when emergencies arise. OTF's rapid response service providers offer assistance with secure and resilient hosting, website audits, forensic analysis of digital attacks, infrastructure improvements, and VPN services. In 2017, OTF provided emergency support for a variety of digital emergencies experienced by high-risk internet users and organizations such as journalists, bloggers, cyber activists, civil society organizations, and human rights defenders.

The majority of support provided through the Rapid Response Fund was in small increments (<$5,000). This allowed OTF to provide direct support to numerous projects while staying below the $50,000 per project limit set for the Fund. Over the years, the Rapid Response Fund has been utilized by entities around the globe, including those focused or residing in Azerbaijan, Burma, Egypt, Iran, Iraq, Jordan, Lebanon, Serbia, Syria, Uganda, Zimbabwe, and many others. In calendar year 2017, OTF received 60 requests for rapid response support and ultimately provided funding for 14 engagements. This was a significant increase in requests for support over years past.



Detailed below are three of the larger dollar value Rapid Response projects from FY2017. To compare, most Rapid Response projects are typically within the range of $3,000 to $15,000 and focus on smaller scale efforts including digital forensics investigations following suspected attack, recovery of compromised sites or accounts, or other forms of urgent digital security support.

### Adversary Lab
**$40,634**

Adversary Lab is a publicly available and open source resource for the worldwide community of internet freedom tool developers. The purpose of this tool is to utilize machine learning to test network traffic to determine its blockability before being deployed in the field. This helps application developers to create applications that are more resistant to network filtering attacks. In particular, applications which use or provide network traffic obfuscation mechanisms can be tested before they are deployed. The results of this test can then be used by tool developers to eliminate these blockable properties from their network traffic. Adversary Lab has been used to analyze the network traffic patterns and blockability of many popular internet freedom tools and network traffic obfuscation techniques. OTF's funding of Adversary Lab allowed it to continue to evolve and analyze more sophisticated attacks in a much shorter time period. This project enhanced the testing platform to reflect the more sophisticated testing approaches recently employed, and also carried out testing utilizing this increased functionality.

### Security for Iran
**$25,000**

The Security for Iran project helped a prominent Iranian human rights organization to implement security improvements to their website and database to prevent further security pitfalls. Without the assistance provided, the community was at risk of being susceptible to phishing attacks and could have become a honeypot for adversaries to digitally threaten a large swath of the Iranian human rights community. Keeping the community's outreach and engagement platforms as secure as possible contributed greatly to the overall digital security health of the community given that Iranian human rights organizations are well-connected with each other and the broader human rights community.

### Cyberwarfare in Kyrgyzstan Elections
**$28,600**

Kyrgyzstan's presidential election is a useful case study for research and analysis on the impact cyber war during an election and identify means to limit the implications. In Kyrgyzstan, media is regarded as Not Free by Freedom House, and government critical media outlets often face hostility and threats from the government. Kyrgyzstan applies selective internet filtering in political and social events, doing so increasingly in recent years. For its presidential election, this project aimed to: 1) ensure that one major independent media outlets remains online, reachable to the local population, and non-compromised during the elections; 2) document and disseminate

cyber attacks and internet censorship against sites of public interest during the election period; 3) analyze and research the source and impact of mis-information (fake news) in social media and traditional online media during the election period.

## Fellowship Programs

In FY2017, OTF funded the Digital Integrity Fellowship Program as well as the Information Controls Fellowship Program.

### Digital Integrity Fellowship

The Digital Integrity Fellowship Program (DIFP) provides fixed monthly stipends to individuals capable of addressing short-term and long-term threats to freedom of expression online. Fellows use their digital security expertise to provide organizations and communities most affected by internet freedom violations with comprehensive internal support. They also 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. Applicants propose the organizations with whom they will work (groups that have experienced threats to their digital security). Fellows receive a $5,000 monthly stipend and a small stipend for equipment and subscription purchases to enhance the security of the organizations with whom they work.

The DIFP welcomed three fellows after receiving 34 submissions in the 2017 application round.

---

Bex Hurwitz

Bex worked closely with a women's human rights defenders network in East Asia to audit and improve their collective digital security practices, helping to find secure ways for their staff to collaborate from multiple locations.

Poncelet Ileleji

Through his partnership with the Gambian YMCA, Poncelet worked with leading Gambian civil society organizations to guide their staff through a series of trainings designed to bolster their IT knowledge, from the most basic digital security practices to long-term digital security strategies.

Stephane Labarthe

Stephane implemented digital security best practices with Karisma Foundation, an NGO based in Colombia working for human rights in internet and IT. Together, Stephane and Karisma created the K+LAB "Digital Security and Privacy Lab" and provided digital security support to six of Karisma's core projects. Stephane was also able to help seven Colombian NGOs strengthen their digital security practices.

Information Ecology

Information Ecology provided mentorship for OTF Digital Integrity Fellows in the successful completion of their projects. Support was provided on technical, strategic, organizational development, and change management topics to ensure fellows were increasing both their own and their affiliated organizations' capacity to successfully undertake security initiatives.

### Information Controls Fellowship

The Information Controls Fellowship Program (ICFP)[58] cultivates research, outputs, and creative collaboration on topics related to repressive internet censorship and surveillance. The program expands collaboration on capacity building as fellowships are hosted at premier organizations and research institutions, including University of Toronto's Citizen Lab, International Computer Science Institute, Harvard University, University of New Mexico, and Coding Rights. 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 $4,200 monthly stipend and a small travel budget that varies based on the length.

The ICFP welcomed eight fellows after receiving 72 submissions in the 2017 application round.

---

Ihsan Ayyub Qazi

*Host organization: International Computer Science Institute, UC Berkeley*

Ihsan significantly advanced the development of an incentive-compatible tool for measuring internet censorship at scale. This project leveraged expertise at the University of California, Berkeley, to assess the tool's security and privacy aspects, and complete its implementation prior to the public release of a beta version. Ihsan used his previous research on the topic (see "A Case for Marrying Censorship Measurements with Circumvention") to bring the concept from theory to practice.

Taha Khan

*Host organization: International Computer Science Institute, UC Berkeley*

As a senior fellow, Taha worked to better understand the commercial VPNs ecosystem, focusing specifically on how they handle user traffic and to what extent these services actually stand up to their public privacy claims. Taha produced a paper and open source code, and created a website based on empirical evidence, which can be accessed by global users to understand the specifics of VPN services and make more informed choices when selecting amongst available VPN services.

[58] OTF's 2017 funding for Information Controls Fellows also included a fellowship which concluded early due to unforeseen circumstances and three fellows from the 2018 class.

Sergei Hovyadinov

*Host organization: Ranking Digital Rights Project, Open Technology Institute, New America Foundation*

As a senior fellow, Sergei worked with the Ranking Digital Rights Project at the Open Technology Institute to provide an in-depth analysis of the role of internet intermediaries in the execution of Russian state controls over the internet, and how these companies adjust their operations and transparency practices in autocratic regimes like Russia. A Russian version of this work was released first, while a summary blog post and the accompanying paper were subsequently released in English. Sergei presented the findings at numerous conferences and other public events and produced two additional blog posts in Russian. Sergei also published a post detailing the gaps in existing transparency reports.

Zack Weinberg

*Host organization: Calipr research group at University of Massachusetts, Amherst*

Zack further developed software capable of continually refining the set of web pages monitored for censorship in various countries, and assisting with analysis of the censorship policies in these countries. Zack also published a paper assessing the geographic accuracy of proxy servers for commercial VPNs. Zach's previous research includes "Topics of Controversy: An Empirical Analysis of Web Censorship Lists."

Igor Valentovitch

*Host organization: Equalit.ie*

Igor conducted comparative research on the growth of information controls in Russia, Belarus, Kazakhstan, Uzbekistan, and the disputed territory of Crimea. He investigated instances of blocking and DDoS attacks against the online platforms of local civil society projects to identify common trends and isolate potent triggers of internet censorship in the region. Igor will release a joint paper with ICPF Fellow Ksenia Ermonshina discussing the filtering of liberal platforms in Russia and Crimea around the presidential elections in March 2018, as well as another paper providing a comparative analysis of information controls across the examined CIS countries since 2014.

Ksenia Ermoshina

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

Ksenia undertook a thorough analysis of informational controls, surveillance, and circumvention tactics in the disputed territory of Crimea. In doing so, she utilized a hybrid methodology combining network measurements, science and technology studies, and a qualitative ethnographic approach. A forthcoming report analyzes three layers of "cyber annexation": infrastructure, censorship and digital security. Ksenia's previous research includes "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era."

Simone Basso

*Host organization: Measurement Lab, Open Technology Institute, New America Foundation*

Simone worked to advance the MeasurementKit platform. MeasurementKit is the engine underneath censorship detection tool OONI-Probe's mobile testing platform and the Measurement Lab network performance testing platform, which generate millions of data points each year. Simone focused on making network performance measurements more easily available on mobile and embedded devices, and on making the engine used by OONI available on Windows and more capable. Simone extracted from Measurement Kit libndt, a small library tailored for the needs of people seeking to integrate NDT, a well-known network performance test. Simone, and his host organization Measurement Lab, also co-designed a better network performance test protocol, called ndt7, that collects more useful low level information building on recent Linux kernel advancements while reducing bandwidth usage. Both ndt7 and the NDT engine extracted from Measurement Kit have been extended to use TLS and WebSockets, allowing them to be more web friendly and more likely to work in mobile environments.

Arzu Geybullayeva

*Host organization: Berkman Klein Center, Harvard University*

Arzu significantly advanced understanding of information controls in Azerbaijan. She performed research around the country's internet infrastructure and relevant country legislation, documenting past internet blocks and surveillance mechanisms used, and tracked network interference. A summary of her research was posted on OTF's website. Arzu's previous research includes "In the crosshairs of Azerbaijan's patriotic trolls."

---

# Labs

Despite the diverse nature of challenges being tackled by those in the internet freedom community, a common set of needs exists when it comes to tools and technologies. These needs include secure hosting, code audits, localization into multiple languages, and help with usability design or event support. Accordingly, in addition to directly funding projects through regular open calls, OTF offers a range of services designed to address these core needs through cost-effective service interventions. These services fall under four labs: the Engineering Lab, the Community Lab, the Usability Lab, and the Localization Lab. By coordinating the provision of these services through the four labs, OTF is able to achieve economies of scale and bring down the overall cost for the internet freedom community. These services are generally available to both OTF-funded projects, as well as other important internet freedom efforts, through applications associated with each lab.

## Engineering Lab

The Engineering Lab houses OTF's technical service offerings, including Eclipsis, the OTF-supported Secure Cloud Infrastructure, Amazon Cloud credits, Google Apps credits, and other engineering resources frequently needed by projects. The lab also includes code security audits (formerly a standalone "Red Team Lab"), performed by a group of highly specialized auditors and pen testers. In FY2018, OTF will expand the Engineering Lab to include developer services to help important information freedom efforts integrate key internet freedom technologies into their projects or tools.

### Eclips.is

**$115,310**

Through Eclips.is, OTF works with partners on the ground to deploy high-capacity cloud infrastructure for use as close as safely possible to high-censorship areas in the Middle East, Northern Africa, and Asia. Once deployed, access to the infrastructure is given to both OTF and non-OTF projects to research, develop, and deploy their tools and services in a secure environment. This results in greater access and lower overhead for projects. As experts in their field, secure hosting provider Greenhost has been contracted to build, maintain, and manage this OTF-funded Secure Cloud initiative. Due to the success of the Eclips.is project, OTF has requested Greenhost split its Service & Maintenance contract from the future development of the Eclips.is platform.

## Community Lab

The internet freedom community, in the most grassroots sense, is comprised of actors around the globe responding to distinct local or national threats. Repressive actors, however, continue to gain strength by learning from global advances in circumvention and surveillance technology. Accordingly, it is vital that those striving to advance internet freedom are able to convene nationally, regionally, and globally to share best practices, discuss emerging threats, and establish networks of support and trust. In FY2017, OTF used the Community Lab to support events focused on regional communities dealing with the challenges of repressive censorship and surveillance in Africa, Latin American, the Middle East, and Asia. More technical gatherings tackling key challenges, such as network and censorship monitoring, were offered as well.

### Internet Freedom Festival

**$250,000**

The Internet Freedom Festival, co-sponsored by the DRL OIF Program, brings together technologists, journalists, rights workers, researchers, advocates, and funders working to advance freedom of the press, expression, privacy, and security in repressive countries around the world. The 2017 event in Valencia, Spain involved 1,300 people from 114 countries and included over 220 sessions.

### Arab Digital Rights Summit
**$40,035**

The Arab Digital Rights Summit (ADS) is an event designed to strengthen and expand the MENA regional community, working to bolster digital freedom in online spaces and fight against increasing government restrictions and surveillance. Held in the fall of 2018 in Beirut, the ADS gathered the MENA regional community in an effort to encourage better coordination across efforts and actors. The event offered opportunities for peer-learning and critical skill-building, as well as new ways to foster trust and solidarity. These efforts are necessary to help communities in the Arab region respond to the most urgent threats to their digital safety.

### Forum on Internet Freedom in Africa
**$48,850**

The Forum on Internet Freedom in Africa is a multi-stakeholder event on protecting and promoting internet rights throughout Africa. It is organized under the OpenNet Africa initiative of the Collaboration on International ICT Policy for East and Southern Africa and the Association for Progressive Communications. The event brings together over 250 thought leaders from 35 countries to discuss the state of internet freedom in Africa. The Forum works to support skills development in digital security practices among civil society organizations, journalists, human rights activists, and other at-risk groups, such as women and the LGBTQI community.

### Primevera Hacker Festival
**$20,000**

The Primavera Hacker Festival is a free, yearly gathering organized in Santiago, Chile, focusing on the relationships between technology, politics, and culture within the Latin American context. The event's target audience includes activists and technical experts focused on the research and development of digital rights and circumvention tools, academics working on digital rights and social movements, and open source advocates. The latest gathering focused on a host of important issues, including identifying better ways to localize circumvention tools for the Spanish-speaking context (with a special focus on the needs of women and LGBTQI communities), and instigating more technology-focused collaborations between organizations and collectives in the region.

### Global Voices Summit
**$54,500**

The Global Voices Summit explores how key ideas in the structure of the internet and the shape of online discourse can rewire our societies for resilience, deliberative civics, and journalism based on cross-cultural understanding and trust. The event brings together the Global Voice community, which includes journalists working in hostile and difficult information environments from the Global South, in an effort to provide digital security training to key stakeholders working in surveilled and censored environments. At the 2017 event, training and analysis took place during

a series of sessions where individuals discussed threats and learned about the installation, practice, and use of specific tools (such as Signal, Wire, GPG, XMPP, VeraCrypt, and Meet.Jit.si).

### Research Methods Workshop for Digital Rights Africa
**$9,171**

The Research Methods Workshop for Digital Rights Africa helps participants learn how to employ a variety of quantitative and qualitative methods. Topics covered by the event include network measurement tools, better security practices, and open source tools for web scraping and social network analysis. Participants learn how to design surveys tailored to specific needs and available resources, conduct expert interviews and focus groups, and communicate information and raw data in compelling ways.

### Iran Cyber Dialogue 2017
**$55,850**

The Iran Cyber Dialogue is an annual hands-on event designed to produce collaborative solutions to promote access to information and enhanced privacy and security for Iranians online. The goal of the event is to improve understanding of issues, develop better resources, and strengthen strategies for better online access to information and freedom of expression.

### Citizen Lab Summer Institute (2018)
**$45,158**

The Citizen Lab Summer Institute on Monitoring Internet Openness and Rights is a series of intensive research workshops hosted annually at the Munk School of Global Affairs. This event is a key event for the information controls research community, including the current class of OTF Information Controls Fellows. In 2018, the workshop saw its highest level of attendance ever, and brought together diverse experts from various disciplines focused on studying technologies and policies that either threaten or promote freedom of speech online. These experts came from various regions and professions, including academic, legal, policy, and civil society. The event focused on four research streams: Network Interference and Freedom of Expression Online, Surveillance and Counter Surveillance, Policy and Transparency, and Security and Privacy of Apps. The knowledge shared at the event allows for the identification and pursuit of future collaborative research projects. A full summary of the event can be found here.

### OONI Gathering 2017
**$41,070**

The OONI project is a free software project that empowers decentralized efforts in increasing transparency of internet censorship around the world. The OONI Gathering 2017, a two-day event taking place just prior to the 2017 Citizen Lab Summer Institute, convened a variety of project partners from around the globe to strengthen partnerships and gain key insights as to how the OONI platform can better assist users. Topics addressed included improvements to usability

through notifications and customization, improved testing for network shutdowns, and ways to improve the ability to generate rapid data analysis. A full summary of the event can be found here.

### OpenNet Africa
### $65,300
The Opennet Africa project works to enhance the digital rights knowledge, digital security, and safety capacity of journalists, human rights defenders, vulnerable women, and LGBTQI organizations in five African countries. This enables these civic actors not only to work securely and effectively to promote human rights, but also become infomediaries and multipliers of digital security knowledge and skills. The project also empowers tech innovators to engage in needs-finding in technology-for-human rights through understanding usability and security vulnerabilities in tools design.

### Mekong ICT 2017
### $40,000
Mekong ICT Camp is a recurring workshop on the topics of information, communication, and technology for citizen media, NGOs, and other influential stakeholders in the Southeast Asia. The event maintains a special focus on the Mekong sub-region countries where people's rights to development remain relatively scarce.

## Usability Lab
**$250,000**

Usability Lab service providers aim to increase user safety and promote practical internet freedom by supporting tool developers in their work to improve the overall user-friendliness and success of internet freedom and human rights technology. In FY2017, OTF expanded the services of the Usability Lab based on feedback from the community in an effort to provide more user interface design and usability testing services, and increase the number of available Usability Lab service providers to address the growing need for usability services.

### Guardian Project/Okthanks
Guardian Project, in partnership with Okthanks LLC, provides secure usability services. Guardian Project specializes in the development of privacy-protecting and security-enhancing mobile applications and tools, with deep experience on both Android and iOS operating systems. Through prototypes and testing, Okthanks creates clear, effective user experiences and brand messages through prototypes and testing, in an effort to make tools simple to use and easy to understand.

### Simply Secure

Simply Secure is a nonprofit dedicated to helping teams make technology that meets user needs for issues of security, privacy, and transparency. Founded in 2014 to support the internet freedom and open-source communities make their tools more usable, Simply Secure offers UX coaching and user-study design, as well as a growing set of online resources.

### Torchbox

Based in the United Kingdom, Torchbox is an award-winning independent digital agency specializing in digital strategy, user experience design, website development, software engineering, and digital marketing. Established in 2000, Torchbox designs and builds responsive websites and applications for some of the world's great universities, think tanks, charities, NGOs, and membership organizations.

### Ura

Ura is a digital agency focusing on visual communication solutions tailored for open source and internet freedom projects. The agency strives to improve usability and experiences by keeping in mind each project's unique community consensus. Founded in Albania in 2016, Ura meets the rising demand for usability and design services in open source software by offering the UX design, design systems research, and visual identity services necessary to support a project's needs.

## Localization Lab

OTF's Localization Lab works to make internet freedom tools and resources relevant, accessible, and more usable for global communities in need. To do so, the Localization Lab creates space for end users, developers, CSOs/HROs, and trainers to communicate by way of localization efforts. OTF supports these efforts by directly supporting the Localization Lab and providing funding for the Transifex platform on which the Lab is run.

### Localization Lab
### $225,500

In 2017, the Localization Lab expanded by 803 contributors, enabled the translation of more than 1.5 million words across 70+ projects, and organized four localization sprints (one international, three regional) in the following languages: Azerbaijani, Burmese, Thai, Bahasa Indonesia, Khmer, Farsi, Spanish, Luganda, Shona, Swahili, Ukrainian, Russian, Turkish, Brazilian Portuguese, French, Gujarati, Kannada, and Urdu.

### Localization Lab (Transifex Platform)
### $461,772[59]

[59] The Transifex platform is renewed on an annual basis. Given the period of time covered by the FY2017 allotment, two years of platform service was paid for with FY2017 funds.

To house and analyze all of the language translation for OTF-funded technology projects, and to make them available in languages other than English, the Localization Lab needs a web-accessible, easy-to-use system to allow translators and technology projects to submit and pull the translations that will be utilized by internet freedom projects. Transifex provides the platform in which language translations can be submitted and managed across projects and individuals.

---

# The OTF Program

The effects of OTF's funding now reach more than two billion users around the world due to a calibrated combination of funding the development of the next generation of user-facing tools, patching key infrastructural vulnerabilities, providing digital security support to the most targeted groups, expanding the reach of successful internet freedom technologies, and supporting cutting edge research.

OTF remains focused on supporting users in the most repressive environments in the world as it continues to expand the reach of internet freedom tools. For those experiencing repressive state censorship and surveillance, OTF's funding process offers a transparent, open, and widely accessible way to create and implement solutions in the fight for internet freedom. To that end, OTF's FY2017 projects, fellows, and lab services supported efforts to aid populations in places facing high levels of state censorship and surveillance such as Tibet, Xinjiang, Crimea, Zimbabwe, and Iran.

## Getting closer to the field

### Raising front-line capacity

OTF has always worked to advance the technological capacity and capabilities of people on the ground in countries with the least legal protections for online expression, speech, and free press because those priority countries are where the most egregious internet freedom violations occur.

Over the past year, OTF moved to further prioritize support for efforts that not only support people living in repressed environments, but which emanate from within those communities. The front lines of censorship change quickly, with adversaries adjusting and recalibrating their efforts in real time. So it only makes sense that the most effective, efficient solutions to repressive censorship should come from the individuals, networks, and organizations experiencing it firsthand. Therefore, in the past year OTF increasingly prioritized funding for applicants who are located within priority countries or who work closely with trusted local groups. In both cases, OTF emphasizes support for the development of tools that are built with direct feedback from target users, such as through collaborative design processes.

Keeping tool development closer to the field helps create more effective, adaptable, and culturally nuanced tools. Recognizing that this shift is a process, OTF worked over the past year to forge connections between disparate groups when appropriate, prioritizing the voice and gains of those on the front-lines. As a result, OTF oversaw a growing number of connections made between technologists, activists, journalists, and other key actors. These connections resulted in an increase in the number of successfully submitted applications from people within priority countries and with more diverse geographic, experience, and knowledge backgrounds.

### Hosting an international summit

OTF's 2017 annual summit, in which all new OTF projects and fellows gathered to learn from one another and help improve OTF, was held in Valencia, Spain. This marked the first time in OTF's history that the annual summit was held outside of the United States and served as an important step in OTF's ongoing efforts to move closer to the communities it supports (Valencia is the site of the Internet Freedom Festival and has been recognized as a safe haven for journalists under threat). The event brought together nearly 200 attendees, including individuals representing OTF-supported projects, OTF fellows, OTF Advisory Council members, funders, and experts from the greater internet freedom community. Participants discussed current and emerging challenges, innovations, strategies, and priority needs in the field of global internet freedom. The 2018 OTF summit occurred in Taipei, Taiwan, furthering these efforts to develop and connect regional communities.

## Improving efficiency, responsiveness, and security for applicants

### Increasing transparency and responsible data handling

OTF took steps in 2017 to increase transparency and share more of what is learned through the application and review process with the internet freedom community. In doing so, OTF worked to protect the sensitive data shared by applicants and commissioned a needs-finding study by The Engine Room to assess the best way to share what is learned while still protecting applicant data. As a result, OTF now has a Responsible Data Policy which is in the process of being implemented.

### Updating our Submission System

In 2012, OTF deployed a working web-based app to accept open submissions. At the time, OTF supported fewer than 20 efforts in an entire year. Five years later, however, the app began to struggle to keep up with OTF's rise in prominence and the evolving needs of the internet freedom community.

Therefore, after an extensive review of similar open- and closed-source solutions, OTF decided to create a new open-source submission system capable of meeting its unique needs of scale, quality, ease of use, and security.[60] Today, all submissions received by OTF are managed by the new app,

[60] https://github.com/OpenTechFund/opentech.fund.

which continues to mature and adapt to the needs of OTF's team, Advisory Council, applicants, and the broader internet freedom community.

## Strengthening donor collaboration

Worldwide, the resources allocated to restricting internet freedom dwarf those put toward advancing it. The funding, manpower, and technologies deployed by authoritarian regimes worldwide for censorship and surveillance purposes are far greater than those put forth by democratic states aimed at expanding access and bolstering digital safety. As it stands, no single source of funds, whether public or private, can provide enough to effectively defeat these powerful censorship regimes. Despite this David vs. Goliath dynamic, the relatively small amount of funding put towards internet freedom has enabled the research, development, and deployment of tools that regularly give millions of people living in repressive societies the ability to access censorship-free networks and communicate more securely. These successes have helped to lower barriers to unlocking additional funding sources, as they have shown that even small seeds can bear impressive, impactful fruit.

Since our founding, OTF has worked to raise awareness among funders about the importance of internet freedom and its fundamental connection to broader human rights issues. We engaged with donors on education initiatives to increase and diversify the support available for internet freedom projects. This has led to the creation of a global network of private foundations, tech companies, startup incubators, like-minded foreign government funders, and venture capitalists committed to advancing global internet freedom. In FY2017 alone, more than 200 individual donors and foundations participated in OTF-supported efforts to address this challenge. Established international events such as the Internet Freedom Festival, RightsCon, MozFest, re:publica, Human Rights Funder Network Global Conference, Funders' Initiative for Civil Society, and many others have become regular meeting points for donors to learn more about internet freedom issues, identify shared interests, and formulate collaborations. By forging these partnerships, OTF has played a key role in unlocking new sources of internet freedom funding.

To ensure well-calibrated donor coordination, OTF continues to actively participate as a trusted advisor in the development of complementary donor initiatives while also participating directly in the review process for certain funders. OTF convenes on a regular basis with complementary US government-funded programs including the U.S. State Department's Internet Freedom Program, USAGM Office of Internet Freedom, and USAID, ensuring that public funds allocated to internet freedom are utilized as effectively and efficiently as possible. OTF has also collaborated with Collaborators have included: the U.S. State Department's Internet Freedom Program, USAGM Office of Internet Freedom, Access Now, Media Democracy Fund, Ford Foundation, Open Society Foundations, MacArthur Foundation, Knight Foundation, Mozilla Foundation, Linux Foundation, Prototype Fund, British Broadcasting Corporation, Deutsche Welle, Swedish International Development Agency, the German Federal Foreign Office, and many others.

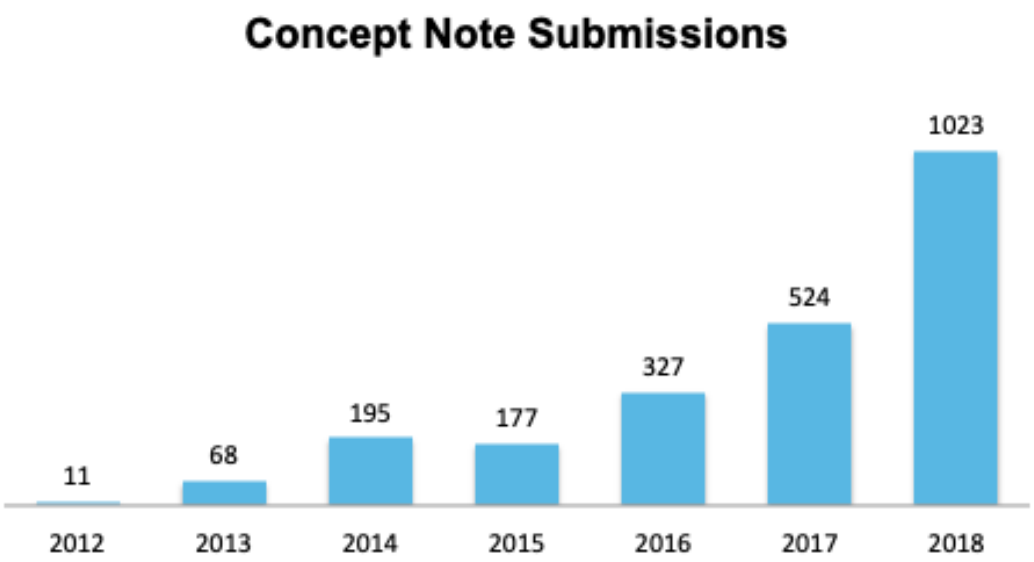
To date, these efforts have helped bring the total amount of private funds dedicated to internet freedom to more than $100 million since OTF's founding. OTF also works to ensure that the internet freedom community is aware of these new funding opportunities, raising awareness by tracking and compiling relevant sources of funding and sharing those with upcoming deadlines, encouraging those with good ideas to investigate the full range of public and private funding sources now available.

Looking to the future, we are excited to see rising donor interest and participation in regional-centric events such as the Forum on Internet Freedom in Africa and the Digital Rights and Inclusion Forum in Sub-Saharan Africa, Bread&Net in the MENA region, and the Mekong ICT Camp in Southeast Asia, among others. The increasing support for such events is indicative of the evolving awareness among funders about the specific issues facing communities on the ground in such locations. When 2018 closes, OTF expects to see an even greater number of engaged donors, more diversity in both funding and approach, and even more funds made available to those advancing internet freedom.

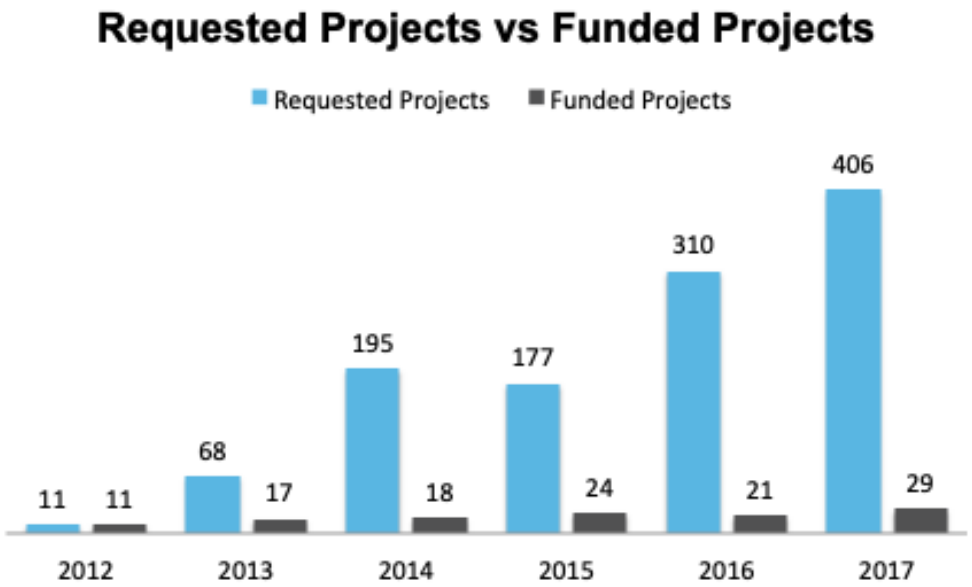
## Operations by the numbers

Perhaps the single most defining feature of FY2017 was the significant increase in requests for support. In 2017 alone, OTF reviewed and responded to over 700 requests[61] for funding (seeking nearly $120 million in total funds). Incredibly, 2018 is on pace to dwarf 2017's figures.[62] This massive increase in requests for funding is an example of OTF's successful outreach efforts to engage new geographies and sub-communities dedicated to the goals of internet freedom. Despite the substantial increase in applications, OTF continues to use the application review process to provide valuable, substantive feedback to those seeking support for their work. When necessary, this feedback includes referring proposals to more appropriate funders.

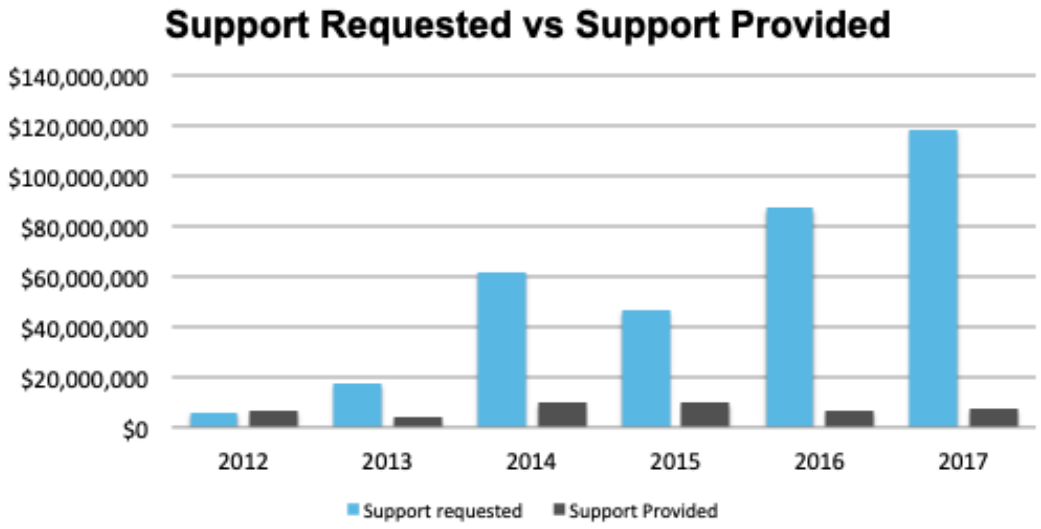
[61] Requests for support include fellowship and rapid response applications as well as applications for lab service support in addition to concept notes submitted to the Internet Freedom and Core Infrastructure Funds.
[62] The number of requests for funding received by OTF in 2018 surpassed the totals from 2017 in July.



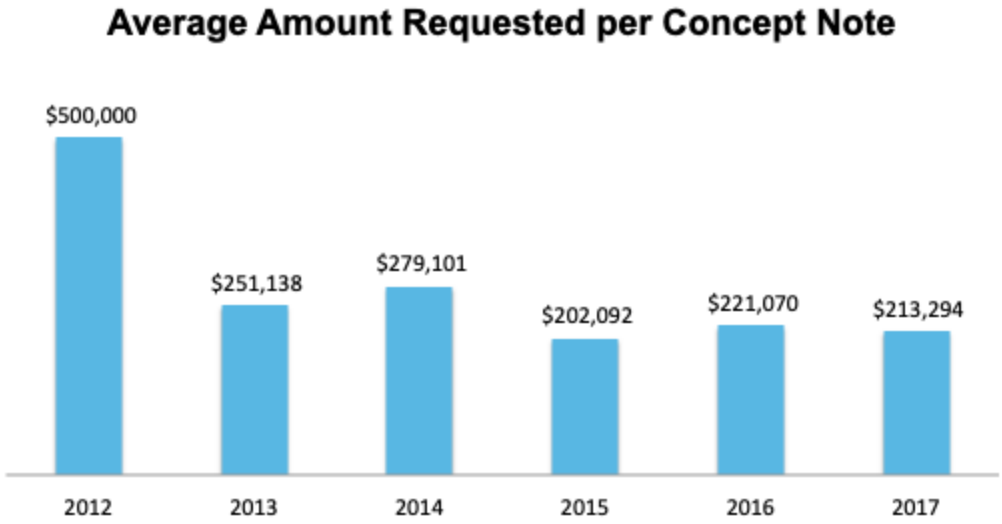

The increase in applications received means that OTF must necessarily fund a smaller percentage of overall applications. As the chart below demonstrates, OTF funding is becoming increasingly competitive.




A similar trend exists with regards to the amount of funding requested and the amount ultimately provided. Applicants requested nearly $120 million in calendar year 2017, far surpassing OTF's $7.285 million in programmatic funding.



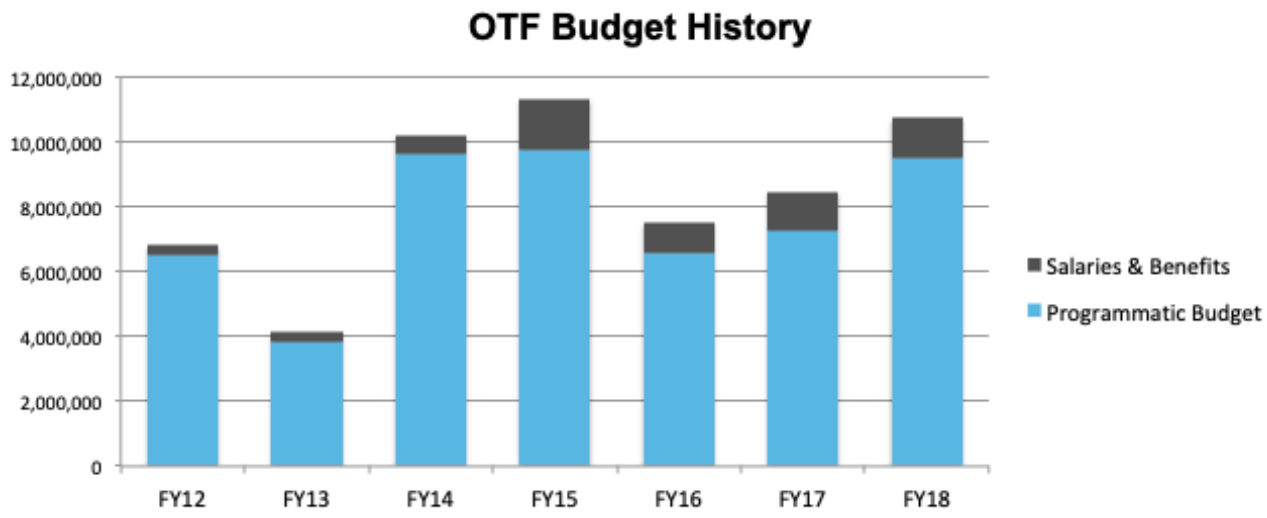

OTF funding supports efforts of many sizes. FY2017 funds went to projects requesting less than $20,000 and to projects requesting more than $500,000. Yet, the average amount of funding requested has been relatively stable in recent years, averaging just over $200,000 per project. Interestingly, the average amount requested is slightly more than twice the average funded project amount in FY 2017 which was approximately $97,000.




## OTF funding

OTF's FY2017 funding allotment totaled $7.235 million in programmatic funds, and $1.2 million in salaries and benefits. OTF's budget comes from the Internet Freedom funds allocated by the United States Congress to USAGM (formerly the Broadcasting Board of Governors). Internet Freedom funds are split between OTF and USAGM's Office of Internet Freedom. The total amount

of Internet Freedom funds allocated to USAGM has remained stable for past three years at $15 million. From 2016 to 2018, however, OTF received an increased share of the Internet Freedom funds. OTF's FY2018 allotment is set at $9.5 million in programmatic funds, and $1.2 million in salaries and benefits.




---

# Fiscal Year 2017 Spending

| **Direct Support** | | |
|---|---|---|
| ***Funds (Projects)*** | | |
| | Internet Freedom Fund | |
| | Awareness | $775,640 |
| | Access | $518,827 |
| | Security | $1,162,753 |
| | Privacy | $173,450 |
| | Core Infrastructure Fund | $450,036 |
| | Rapid Response Fund | $112,364 |
| ***Labs*** | | |

| | | |
|---|---|---|
| | Community Lab | $327,547 |
| | Usability Lab | $250,000 |
| | Localization Lab | $687,252 |
| | Engineering Lab | $158,372 |
| ***Fellowships*** | | |
| | ICFP Class 2017 | $415,500 |
| | DIFP Class 2017 | $238,200 |
| | ICFP Class 2018 (partial)[63] | $166,200 |
| ***Convenings*** | | |
| | Conferences[64] | $250,000 |
| | Summit 2017 | $145,835 |
| | Summit 2018 | $124,522 |
| | Contractor travel | $211,262 |
| **Program Operations** | | |
| | Application System Rewrite | $579,297 |
| | Non-salaried team and consultants | $244,600 |
| | Team travel | $82,503 |
| | Team support | $12,000 |
| | Admin and other | $102,453 |
| | General and other | $10,740 |
| | Office space in DC | $35,646 |
| **Totals** | | |
| | Direct Support | $6,167,760 |
| | Program Operations | $1,067,239 |
| | Total Programmatic Spending | $7,235,000 |

[63] Three fellows from the 2018 ICFP class were funded with FY2017 funds. These work of these fellows will be presented in subsequent annual reports.
[64] This represents OTF's support for the Internet Freedom Festival, which is co-funded by the State Department's Bureau of Democracy Human Rights and Labor.

| | | |
|---|---|---|
| | Designated for Salary and Benefits | $1,200,000 |
| | Total Spending | $8,435,000 |

# Looking to the Future

The internet freedom landscape is marked by constant change. Repressive actors are constantly advancing their ability to censor content and surveil citizens. The internet freedom community is always working to create new ways to circumvent that censorship and keep people safe online. And all the while, the actions of major technology corporations, civil society, and other actors are influencing the landscape as well—with effects both adverse and beneficial.

In such a dynamic environment, a combination of programmatic agility, adaptation, and evolution is necessary for OTF to continue to successfully advance internet freedom around the world. OTF must therefore always look to the future. In doing so, four thematic areas loom largest: (1) the further centralization of the internet and the impact of this on censorship; (2) the need for a more diverse range of circumvention tools to combat the advanced capabilities of sophisticated censors; (3) the need to consider evolving censorship capabilities, such as those reliant on artificial intelligence, in real time; and (4) the continued need to recognize the value in placing priority on technologies built and used by those closer to the front lines of repressive censorship.

## Decentralizing the internet

The internet has gradually become more centralized as people rely on an increasingly concentrated set of infrastructure, services, and applications. Initially a boon for internet freedom defenders, this increasing centralization has more recently become an important factor in shaping the fight between censors and internet freedom advocates. This evolving dynamic can be seen through the relationship between internet freedom and large, multinational corporations.

For years, the infrastructure of large cloud providers enabled "domain fronting," an effective censorship technique which succeeded because traffic emanating from the likes of Google and Amazon was, essentially, too big to block. Faced with the choice of blocking all or none of the traffic from these companies, many authoritarian actors chose to block none. In turn, the centrality of these large cloud providers allowed otherwise blocked traffic to piggyback out of repressive areas.

But in the span of a few weeks in the spring of 2018, anti-censorship tools lost this effective circumvention technique when major cloud providers Google and Amazon made changes to their platforms that rendered domain fronting inoperable. In an instant, one of the most effective circumvention techniques was gone—demonstrating the inherent danger in relying on the whims of large, multinational corporations to advance internet freedom. In this case, the interests of these actors were simply not aligned with those of global human rights defenders, making clear that the latter must be wary of the extent to which the former are relied upon. As demonstrated here, failing to do so can result in serious setback.

The impermanence of domain fronting as a long-term strategy makes plain the need for readily accessible decentralized solutions that feature more independent autonomy than prior techniques. Even though commercial interests have not yet fully aligned for the widespread adoption of decentralized technologies, OTF continues to see promising privacy, resiliency, and anti-censorship possibilities in a future with more decentralized applications. Since its founding, OTF has invested in decentralized technologies. As this field continues to mature, future internet freedom defenders will have the opportunity to achieve success by leveraging the proliferation of powerful mobile devices, the growing maturity of decentralized applications, the increasing ubiquity and utility of encryption for communications privacy, and the growing appreciation for open-source solutions.

Over the next year, OTF expects to see even more applicants request support from the Internet Freedom Fund and the Core Infrastructure Fund to address internet centralization challenges. In addition, OTF will launch an incubator called the Community Prototype Fund, which will support the rapid development of innovative, viable, and open internet freedom technology prototypes to serve the immediate needs of the internet freedom and human rights communities. This fund will join OTF's existing funding mechanisms to provide further support in bringing about internet decentralization. In this manner, OTF will continue to lay the groundwork necessary for a more decentralized internet, while ensuring that technological limitations are addressed and advancements are made with people in repressed societies in mind.

## Expanding anti-censorship capabilities

Over the past six years, the information controls utilized by repressive governments to censor citizens have evolved from a small number of relatively simple, blunt techniques to a multitude of sophisticated, targeted methods. Older censorship approaches that can be more easily detected, such as internet shutdowns, IP blocking, and URL filtering, have been augmented with more advanced and targeted controls. These new controls include content filtering and manipulation, widespread propaganda and astroturfing, and the spread of misinformation. Gains in computing power, storage capacity, data collection, and machine-learning have aided these new censorship methods, as has the growing number of internet-connected citizens who lack both legal and technical privacy protections. Together, these factors have facilitated rapid advances in both automated and human-assisted information controls.

In China, for example, censorship no longer simply entails blocking access to certain apps during politically sensitive times. Now, should an individual share a message containing a banned word or term, automated content moderation algorithms can flag the message and user account for human reviewers to examine. Teams of human censors can then be tasked to infiltrate group chats to spread counter-narratives and intimidate those expressing dissenting views, thereby encouraging self-censorship. Censors can also delete posts, ban accounts, and block access to websites, creating a censorship environment unprecedented in terms of coordination and scale. Such broad-reaching, multifaceted tactics are increasingly common—though their success rate vary

from country to country. Although China is currently the most effective censorship regime on the planet, other like-minded regimes may soon achieve similar censorship success.

Anti-censorship capabilities need to expand now that traditional circumvention technologies can no longer address the full arsenal of modern threats facing free expression, speech, and press online. Current internet freedom communities lack sufficient capacity in areas vital to creating tools and combating threats. These areas include data science, quantitative analysis, machine learning, and cryptography. It is therefore necessary to expand internet freedom approaches by supplementing circumvention tactics centered on end-users with tactics that occur further upstream, such as interventions and technical fixes that publishers, service providers, and content hosts can implement at scale. OTF hopes to see more of these capabilities developed through the Information Controls Fellowship Program, which provides ground-level research findings; the Engineering Lab, which provides insights on the implementation of mature anti-censorship technologies; and the new Community Prototype Fund, which will help those with the most novel, experimental ideas get their projects off the ground.

## Meeting evolving threats head on

A cornerstone of OTF's internet freedom approach is the technical preeminence of U.S. and U.S.-allied technology expertise in internet freedom-related disciplines. In the six years since OTF's founding, the United States has remained a leader in its ability to foster the creation of innovative technologies. But globally, adversaries are starting to catch up, develop, and implement next-generation surveillance and censorship technologies to further erode human rights.

The profound effect of the artificial intelligence (AI) revolution in China is a prominent example of this trend. While the West continues to lead the way in research efforts exploring what AI might theoretically make possible, China is setting the pace in terms of actual implementation, deploying novel AI experiments to see what works in practice. In doing so, China has embarked upon a strategy to reshape the internet to suit its needs. China's country-wide AI strategy calls for the country to lead the world in AI by the year 2030.[65] Attempts to see this strategy brought to fruition stand to further enable the government to develop the technical skills needed to repress internet freedom domestically while also enabling more offensive, outward-facing capabilities. Threats enhanced by these developments include weaponizing the world's online population for massive DDoS attacks, launching more sophisticated phishing attacks, deploying malware at scale and in targeted attacks, and infiltrating hardware supply chains. Inside China, these new tools of repression have already been deployed in an uneven fashion, often leaving citizens guessing as to what level of threat they may be facing.

And as the censorship capabilities of repressive actors like China grow, citizens are facing increasingly harsh consequences for attempting to circumvent state controls. Circumventing the

[65] Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," *New York Times*, July 20, 2017, <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>.

Great Firewall to gain unrestricted access to the internet in China now exposes individuals in the country to a growing arsenal of counter-attacks, whether they be technical, social, or legal in scope.

Given the rate at which these threats are evolving, OTF is committed to supporting the development of tools capable of meeting them head on. The same advancements that are making these repressive technologies possible are also driving innovation in efforts to counter them. Forensic research makes it easier to discover and attribute phishing attacks, analyze malware faster, share threat information, detect censorship events, and discover misinformation sources and minimize their effects. Now, in addition to spotting threats, it is also possible to deploy remediation updates and other machine-assisted techniques with previously unseen efficiency.

Going forward, therefore, OTF will continue to rely on those supported through efforts like the Digital Integrity Fellowship Program to act as a bridge in bringing these skills and know-how to the most at-risk, on-the-ground communities. OTF's Rapid Response Fund will continue to quickly evaluate and introduce new services to effectively counter emerging threats as they arise. The Red Team Lab will continue to ensure the tools and technologies relied on by the internet freedom community are as secure as possible. And the Engineering Lab will steadily roll out support for communities to deploy the most mature, trusted solutions to defend against heightened technical attacks.

## Deepening OTF's front-line stance

When considering the long-term sustainability of protecting and advancing internet freedom, OTF believes the best solutions tend to emanate from within the specific communities where threats are occurring. Homegrown solutions tend to better internalize the local needs, wants, and nuances at play, allowing the tools they create to earn the trust, respect, and use of those who need them most. In addition, front-line technologists are able to observe local preferences and make quicker adjustments.

Significant advances, in terms of technical capacity, are occurring in on-the-ground internet freedom defender communities—enabling greater, more sustainable change. OTF prioritizes applicants who are either from communities affected by censorship or have direct collaboration with such groups. This preference has raised the bar for all applicants, as a successful application for funding now requires not only technological expertise but also the ability to assess the effects of proposed tools on the front-line communities using them. Now the most competitive submissions OTF receives come from within repressed communities, where applicants are developing the tools needed to overcome the repression they themselves are experiencing.

Going forward, OTF will continue to rely on insights gleaned from new and ongoing initiatives to better understand the most pressing challenges and opportunities facing the development, implementation, and continued use of internet freedom technologies in affected communities. Through the Internet Freedom Fund, Core Infrastructure Fund, and the Digital Integrity and

Information Controls Fellowships, OTF will continue to evaluate new and ongoing efforts and adjust accordingly. At the same time, new initiatives like the Learning Lab will help OTF gain a deeper understanding of the front-line efforts it supports. Existing Labs will benefit from increased capacity, allowing the Localization, Usability, Legal, and Community Labs to provide bolstered, direct support for the communities OTF serves. In addition, OTF is exploring a more defined regional strategy, including further diversification of perspectives and experience on the Advisory Council. As a result, OTF expects the coming year will bring forth new initiatives, changes to existing ones, and improvements to all of its various funding mechanisms.