OPEN TECHNOLOGY FUND

FY 2024

ANNUAL REPORT

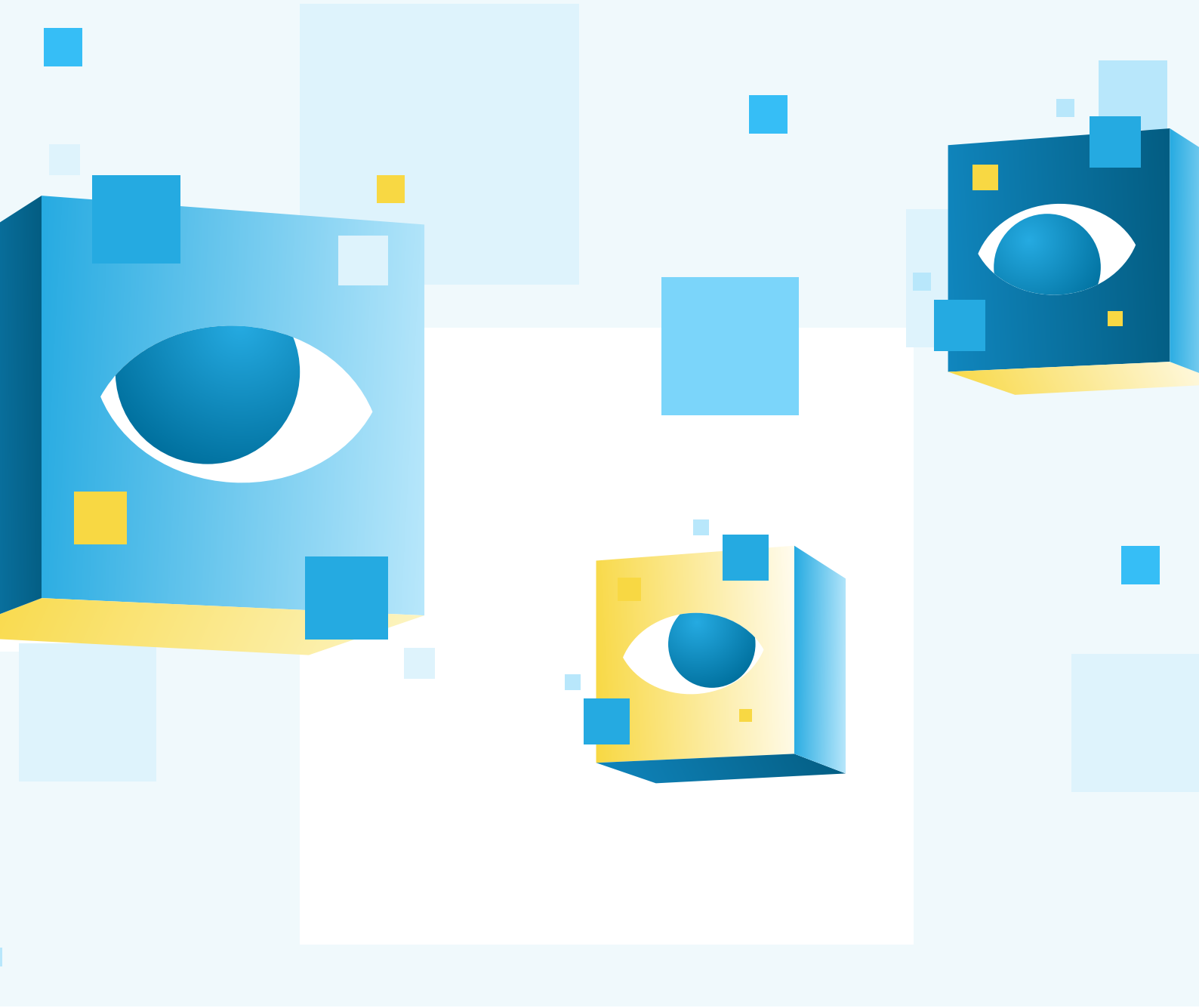
Table of Contents

Layout design and illustrations by **Ura Design**

OPEN TECHNOLOGY FUND

Learn more about OTF at **opentech.fund**.
Follow us on X (formerly Twitter), LinkedIn, and Bluesky.

@OpenTechFund **@Open-Technology-Fund** **@opentechfund**



01 About this Report

This report covers all activities supported by Open Technology Fund (OTF) with funds from the fiscal year (FY) 2024, with the exception of a small number of activities undertaken by highly sensitive projects. The majority of the activities outlined below took place between January and December 2025.

02 About OTF's Mission & Impact

OTF is a congressionally authorized, independent nonprofit organization that advances internet freedom in repressive environments by supporting the applied research, development, implementation, and maintenance of technologies that provide secure and uncensored access to the free and open internet. For over a decade, OTF has supported pioneering open source internet freedom technologies that counter authoritarian information controls and enhance digital security and privacy so that all people can exercise their fundamental human rights online.

Today, **over two billion people** around the world use OTF-supported technology on a daily basis, and **more than two-thirds of all mobile phone users** have OTF-incubated technology on their devices.

2 Billion

people using OTF-supported technology daily.

2/3

mobile phone users with OTF-incubated technology.

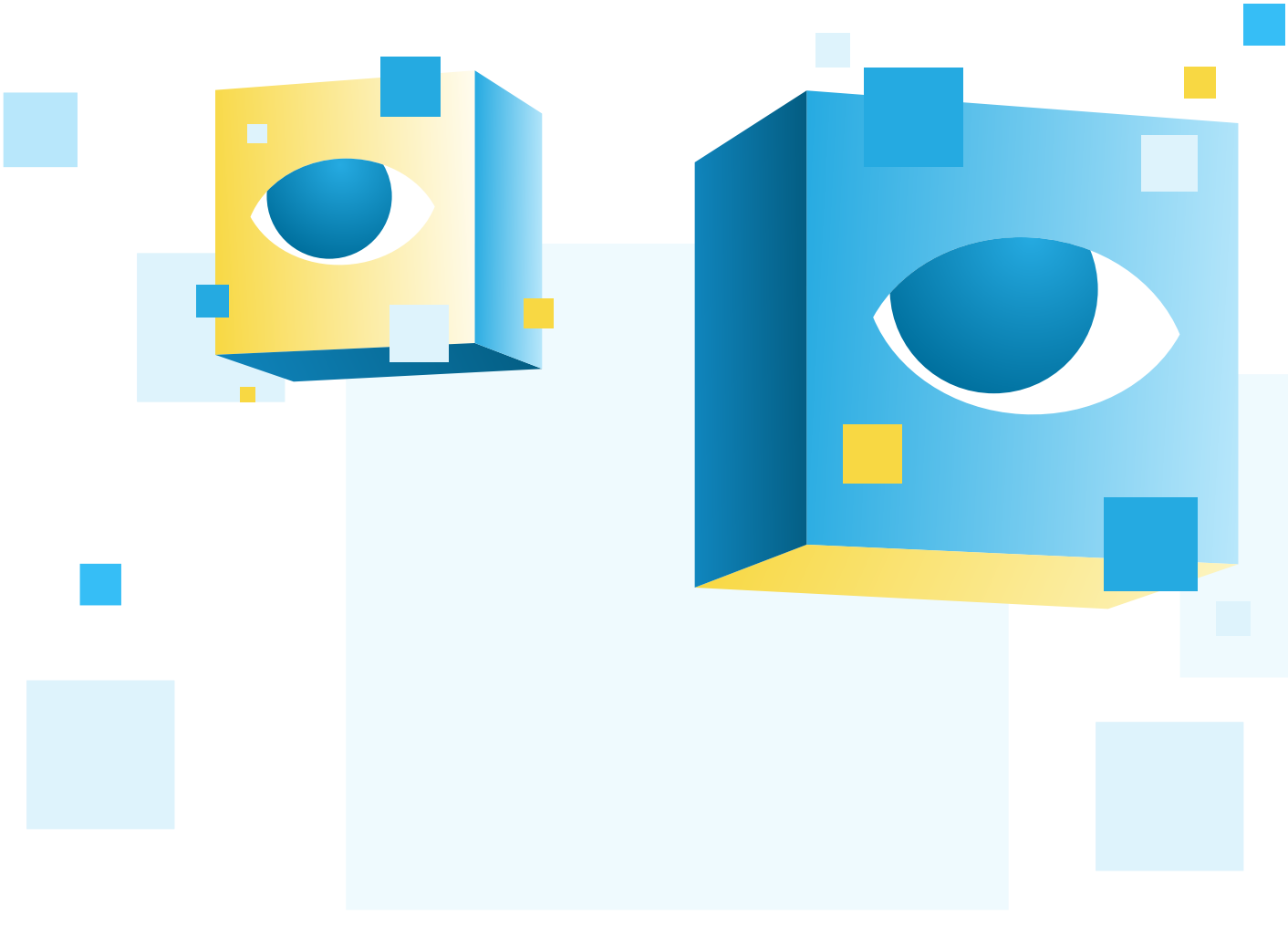
OTF supports projects to:

- **Provide safe, unrestricted access to the internet to individuals living in information-restricted countries.** This includes support for the development and deployment of circumvention technologies that counter increasingly sophisticated authoritarian censorship; the incubation of new solutions to mitigate against internet shutdowns; and the advancement of applied research to help tool developers and users stay ahead of new forms of information control.
- **Protect individuals and organizations from state-sponsored surveillance and digital attacks to ensure they are able to safely access and share information online.** This includes support for the development of secure communication tools and other forms of privacy- and security-enhancing technology, and targeted digital security interventions.

03 Annual Budget

OTF is funded by Congress via a grant from the U.S. Agency for Global Media (USAGM), detailed in a provision in the Department of State, Foreign Operations, and Related Programs appropriations legislation. This legislation requires the submission to Congress of an Internet Freedom Spend Plan outlining the proposed use of appropriated internet freedom funds prior to implementation.

In FY 2024, Congress allocated $94 million for programs to promote internet freedom globally. Of this amount, **$43.5 million was designated for OTF**. OTF's FY 2024 budget allocation reflects a bipartisan recognition of the importance of OTF's work in advancing internet freedom in repressive environments and securing digital rights around the world.



04 Approach to Funding

OTF provides direct funding and support services to individuals and organizations around the world that use technology-backed solutions to address threats to internet freedom.

Internet censorship technology and tactics are constantly evolving. In response, OTF receives, reviews, and contracts projects on a rolling and competitive basis via public open calls to best respond to this changing context.

Funding determinations are made as a result of a rigorous multistage process, through which successful applications are ultimately improved and refined. All proposals are reviewed by OTF staff with subject matter expertise, as well as by OTF's Advisory Council — a volunteer group of technical, regional, and specialized experts from a wide range of relevant disciplines — who provide further feedback and guidance. In addition to ensuring that the most competitive and impactful projects are funded, this multistage review process contributes to efficiency, collaboration, as well as economies of scale. This results in substantial savings of public funds and mitigates against illicit use.

Recipients include qualified technologists, cutting-edge researchers, and digital security specialists, many of whom work in restrictive funding contexts or are at risk due to the nature of their work. While maintaining a high degree of due diligence, OTF offers assistance to internet freedom projects through tailored, cost-effective mechanisms that reduce barriers to funding access.

All prospective projects undergo a compliance evaluation to ensure they adhere to U.S. government requirements for federal funding, including sanctions and other restrictions in authoritarian contexts.

OTF's funding approach ensures that the most competitive projects with the greatest potential for impact are supported. This approach is responsive to the specific funding needs of those projects, and strong due diligence ensures U.S. public funds are effectively spent.

05 OTF Funds, Labs, and Research Program

OTF implemented a number of funds, and resource labs, as well as a research program, in 2025 to fulfill its Congressional mandate in support of global internet freedom.

Funds

OTF provided direct funding to support the applied research, development, implementation, and maintenance of technologies that counter digital authoritarianism in the most information-restricted environments. OTF managed multiple funds that provided resources to innovative global internet freedom projects, large-scale circumvention and privacy-preserving communications technologies, and emergency support mechanisms. These funds included:

Internet Freedom Fund

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

Surge and Sustain Fund

The Surge and Sustain Fund supports millions of monthly active users of large-scale circumvention tools in China, Cuba, Iran, Myanmar, and other authoritarian contexts to safely access the free and open internet. By exclusively funding the user carrying costs of established circumvention providers, this Fund is maximizing the global availability of these tools as demand surges.

Rapid Response Fund

The Rapid Response Fund provides emergency support in response to state-backed digital attacks. Direct funding and support services help those targeted regain online access, mitigate future attacks, and combat sudden censorship events.

Free and Open Source Software Sustainability Fund

The Free and Open Source Software Sustainability (FOSSS) Fund, established with matching support from the public and private sectors, ensures that free and open source internet freedom software projects have the resources and support needed for long-term maintenance.

Resource Labs

OTF provided expert services — solicited on a competitive basis — to internet freedom projects through Resource Labs (Labs), which included the Security Lab, the User Experience & Discovery Lab, and the Impact & Engagement Lab. Together, these Labs supported the security, usability, and adoption of internet freedom technologies.

Security Lab

The Security Lab conducts independent security audits of internet freedom technologies to ensure they are as secure as possible for users in repressive contexts. The primary work of this lab is reviewing and responding to security issues in internet freedom software and tools.

User Experience & Discovery Lab

The User Experience & Discovery Lab improves the usability and accessibility of open source circumvention and privacy-preserving technologies, which contributes to their adoption in authoritarian contexts. Services include secure usability and accessibility coaching, consultation, and audits.

Impact & Engagement Lab

The Impact & Engagement Lab helps technology-focused internet freedom projects effectively communicate about their work in order to contribute to audience adoption in the world's most information-repressive contexts. This Lab also shares knowledge created through projects so others can iterate and build on their work to advance internet freedom.

Research Program

OTF supports cutting-edge applied research investigating tactics and responses to digital authoritarianism through the Information Controls Research Program. This program also contributes to the cultivation of the next generation of digital rights experts by creating a career track for those who have the skills and passion for work towards internet freedom.

Information Controls Research Program

The Information Controls Research Program (ICRP) supports research examining how authoritarian governments restrict the free flow of information online and the solutions to overcome these evolving and repressive tactics.

06 Threats to Internet Freedom

For the 15th consecutive year, global internet freedom declined. The acceleration of this decline in online freedom of expression and access to information is largely a product of China's decades-long socio-technological project to fundamentally reshape not merely what its population sees and says online, but what more than one billion people *think*.

Most of the world does not yet understand the way China's internet works and the global scale of China's online information control ambitions, frequently maintaining an outdated conceptualization of the Chinese Communist Party's (CCP) censorship model as merely a "Great Firewall." However, this vision is technically and behaviorally incomplete at the domestic level where China has quietly pioneered a powerful, new, systemic approach to digital information control. Internationally, China is already exporting components of this model — and the specific technologies that underpin it — to established and nascent authoritarians, fueling transnational repression and enabling new forms of malign political control through meta-censorship and greater internet fragmentation. Its export of both technologies and norms now allows even the most modestly resourced autocrats to cheaply and easily implement population-scale information controls.

From a technological and implementation perspective, the solidification and increasing authoritarian adoption of what researchers are calling the "Locknet" constitutes the greatest single threat to internet freedom today. This singular focus in this report is not meant to diminish the increasing harm caused by the growing prevalence of online censorship, internet shutdowns, domestic and transnational surveillance, and other tactics that are chipping away at freedom of online expression. Instead, it contextualizes these within an emergent authoritarian playbook that, left unchecked, will result in lasting changes to the global internet's digital infrastructure, effectively degrading its free and open future.

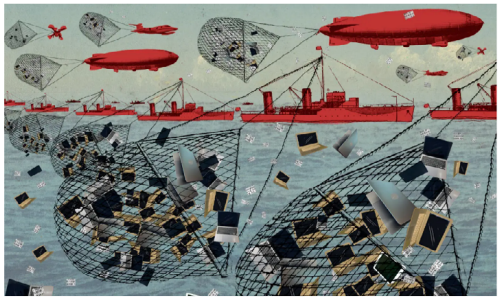
From a technological and implementation perspective, the solidification and increasing authoritarian adoption of what researchers are calling the "Locknet" constitutes the greatest single threat to internet freedom today.

China's Digital Authoritarianism

Over the last decade, the Chinese government has deliberately redesigned their domestic internet to create an unparalleled system of information control. This powerful new model for modern online authoritarian governance simultaneously enables totalitarianism while exploiting the economic benefits of access to the free and open internet. It is the first fully functional alternative to the democratic vision of the global internet presented by its original architects over half a century ago.

It had generally been believed — *until now* — that a country could either be connected to the global internet in a meaningfully fulsome way for social and economic gain; *or* it could erect a "splinternet" which, to achieve comprehensive domestic control, would forgo those benefits. In China's specific case, observers worried for years that the CCP would choose the latter path, creating separate online protocols and services that would sever its domestic internet from the rest of the world. Instead, the CCP rejected the premise of this traditional dichotomy and created a system of overlapping, reinforcing censorship mechanisms that — while individually imperfect — combine to effectively limit what Chinese users can access on the internet without disconnecting from it. As a result, China created a *de facto* splinternet that successfully links up with the global internet.

In the first comprehensive technical analysis of this new model, Jessica Batke and Laura Edelson explained the momentous paradigm shift brought about by the CCP with respect to information control. Far more than an advanced firewall, their system is a multi-level, overlapping, self-reinforcing "Locknet." It provides the Chinese government with unprecedented power to keep out foreign political and cultural influence, and restrict and monitor online life. It does this while simultaneously facilitating China's global influence and commerce like any well-connected modern economy.



Steven Weinberg for ChinaFile

THE LOCKNET

The Locknet: How China Controls Its Internet and Why It Matters

The Locknet

The Locknet is a gauntlet of censorship mechanisms that do not just keep external information out; they also enable the curation of an entirely alternate information landscape that is nearly invisible to users. Through a combination of **service-level censorship** (surveillance that companies must carry out on their own platforms at the government's behest), **network-level censorship** (the inspection and blocking of internet traffic crossing national borders), and **offline compulsion** (regulations, punishments, and social pressures), the Chinese government has created a complex socio-technological system of unparalleled control.

One of the Locknet's central, reinforcing features is aggressive censorship related to knowledge of circumvention techniques and the means to acquire them. This "**meta-censorship**" includes tactics such as ensuring private companies do not offer circumvention tools in their application (app) stores, and censoring discussion of circumvention on social media platforms. As a result, even those in China who want to seek out information on the global internet find it nearly impossible to acquire the tools to do so.

This behavioral element of the Locknet is intentional. Beijing has systematically sought to censor not only specific content, websites, apps, and tools, but to obscure entirely the online world outside the Locknet and any means to access it. These efforts aim to erase the functional memory of what is available beyond the Locknet and replace this with well-curated, engineered satisfaction. The CCP has therefore correctly hypothesized that as functional memory fades, so does the motivation to question the Locknet's boundaries and what may be outside its brave new world.

An Evolving Internet Freedom Model

Over the last decade, the "cat and mouse" game of internet freedom has remained fundamentally unchanged: authoritarian regimes have developed and implemented increasingly aggressive information controls; and, in response, civil society has created and adopted increasingly sophisticated censorship circumvention solutions and privacy-enhancing communications tools. This escalatory pattern has remained relatively consistent and holds true even in countries considered to have advanced internet controls, like Russia and Iran. In both, their populations are willing and able to access circumvention technologies that they then use to interact with a wide array of global platforms and information.

Internet freedom solutions have generally been developed based on an assumption that overcoming censorship is simply a technical impediment that once addressed, will meaningfully restore free, online expression. However, the Locknet's multi-level technological approach, combined with sociological dimensions, means that the traditional internet freedom assumption no longer holds. It is no longer enough to simply make a given piece of content available, because the average internet user in China lacks the knowledge and motivation to discover it. Instead, we need new, creative solutions to address both the technological and behavioral elements of the Locknet.

The Locknet Abroad

The Chinese government is not simply constructing the Locknet for domestic control. Much like the CCP's economic and foreign policies, the Locknet is an exportable commodity used for geopolitical leverage to both influence and undermine the prevailing, liberal rules-based international order.

Russia's Tightening Information Controls

Even before the official start of the "no limits partnership," the Kremlin has been a primary beneficiary of the CCP's information control practices. Previous media reports have shown that Russian officials asked their Chinese counterparts technical censorship questions as the country's media landscape was deteriorating. Since then, the Kremlin has pledged more than half a billion U.S. dollars to upgrade its information controls and further disconnect from the global internet.

As a result of the 2019 "Sovereign Internet" Law, state internet service providers have taken over more than half of Russian IP addresses, consolidating them in the hands of seven state-tied internet service providers, leading to a decrease in the overall number of providers.

The government also created a national domain name system, which works as the internet address book, and government transport layer security certificates, which verify that a given website belongs to a trusted entity and that a user's connection to it is encrypted.

More than blocking specific sites, the Kremlin is following in the CCP's footsteps, using a legalistic framework to criminalize VPNs and other circumvention tools and demand their removal from app stores. In 2024, Apple removed over 50 VPNs at the request of Russian authorities on the basis that these violated local law. In a similar vein, the Kremlin used comparable methods to pressure popular foreign hosting providers and content delivery services to comply with its censorship regime.

In 2024, Apple removed over 50 VPNs

at the request of Russian authorities.

Other authoritarian regimes are not simply importing censorship capabilities pioneered in China, but also learning from the power of the Locknet as a model. One key element of the Locknet's success has been the "WeChat-ification" of online life in China. Intentionally coalescing huge portions of economic and social activity on one domestically controlled platform has paid huge information control dividends to the CCP. The Kremlin is now attempting to replicate that strategy in the form of MAX, a prospective domestically-controlled "super app" that Russian authorities are pushing to achieve market dominance.

The curtailing of Russia's section of the internet into a tightly controlled and isolated forum, combined with the implementation of the domestic messenger app MAX, illustrates the Kremlin's will and technical capacity to adopt the CCP's Locknet model of total internet control. With MAX, the Russian government can capture its citizens on a single app and leverage backend control to censor and surveil them far more effectively, which serves to teach and reinforce self-censorship — a key aspect of the Locknet.

Simultaneously, the app provides all the information and services a citizen "should" need, thereby prescribing the bounds of what is permissible. When this is layered with significant impediments to accessing the global internet or non-state platforms such as censorship, meta-censorship, legal consequences, and offline compulsion, the stage is set for nearly complete information control. Moreover, if this model of control is successfully implemented over a long enough period of time, it is likely to fundamentally re-engineer how Russian citizens think about, search for, and engage with independent information.

> **Currently, the population of Russia still remembers how to access independent information and connect with the wider world. However, as we have seen in other contexts under longer-term heavily imposed information controls, they risk losing this memory the longer government censorship remains unchecked.**

Authoritarian Learning

The spread of the CCP's draconian information controls is not contained to Russia. We are witnessing the rapid acceleration of digital authoritarianism in other countries, too — largely attributed to autocratic learning. Authoritarians are increasingly iterating on and sharing censorship and surveillance techniques and technologies with one another. For example, new research from OTF-supported digital forensics lab InterSecLab and their partners show how the Chinese government's repressive information controls are now an exportable commodity.

Their report, *The Internet Coup*, documents how Chinese company Geedge Networks is selling a comprehensive system with China's Great Firewall capabilities to governments worldwide, including Ethiopia, Kazakhstan, Myanmar, and Pakistan.

Similarly in Iran, Chinese companies — driven by profit motives, yet empowered with CCP state norms — are providing the technologies that the Iranian regime uses to undermine free and open networks in a piecemeal fashion. Reporting shows that ZTE, Huawei, and other companies are providing Iran with sophisticated surveillance and censorship technologies, and are informing Iran's evolving digital isolationist approach to internet governance. Notably, the Iranian government has praised China's "cyber sovereignty" doctrine, and has relied on its economic and political relationship to structurally and politically mimic this as an alternative to a free and open internet.

The Locknet's Global Impact

China's online censorship is quickly creeping beyond its own borders as the CCP is leveraging the Locknet's interoperability with global networks to advocate for new internet standards that would enable greater surveillance and control. By ensuring that new global standards do not prioritize privacy and security — by design — the CCP can make its domestic control even more effective. They can soften the ground for broader global adoption of similar information control strategies, all while remaining connected to global networks.

For instance, in April 2025, the Cyberspace Administration of China published a report detailing how it would promote its internet governance model both domestically and internationally as one that is more favorable than the traditional conception of the global internet.

In other instances, Beijing's network-level censorship is seeping into international internet traffic unrelated to China. For example, Chinese platforms like WeChat that are widely used internationally often replicate Chinese censorship abroad without users' knowledge. In some cases, international companies even willingly reproduce Chinese censorship, incorporating censored large language models into their global products. As a result, even without setting foot in China, internet users around the world — *including American citizens* — are now subject to China's censorship dictates.

Looking Forward

To be clear, the CCP's pioneering transition from employing a collection of individual censorship tactics to a new, fully functional, integrated model of internet control should be understood as a breakout moment. While the Chinese government successfully constructed the Locknet with little notice from the rest of the world, we must now engage with its reality and understand the CCP's online ambitions within it. China's future and the Locknet are now inextricably linked, and as such we must reckon with it, both as it exists within the mainland and as it projects out into the rest of the world.

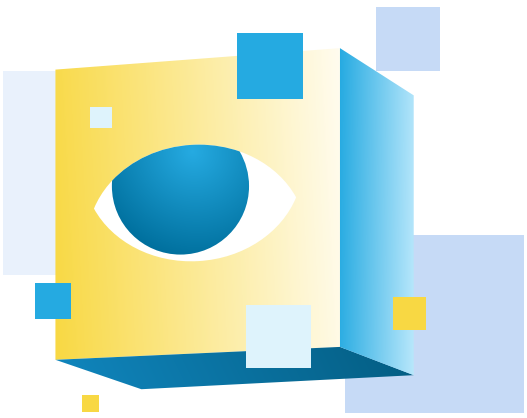
Contending with this reality will require the introduction of new technologies and tactics to deconstruct the layers of the CCP's online control, and re-expose direct linkages to the open internet for people in China. While traditional circumvention solutions remain important, the Locknet model presents a number of novel challenges that must be met with new approaches.

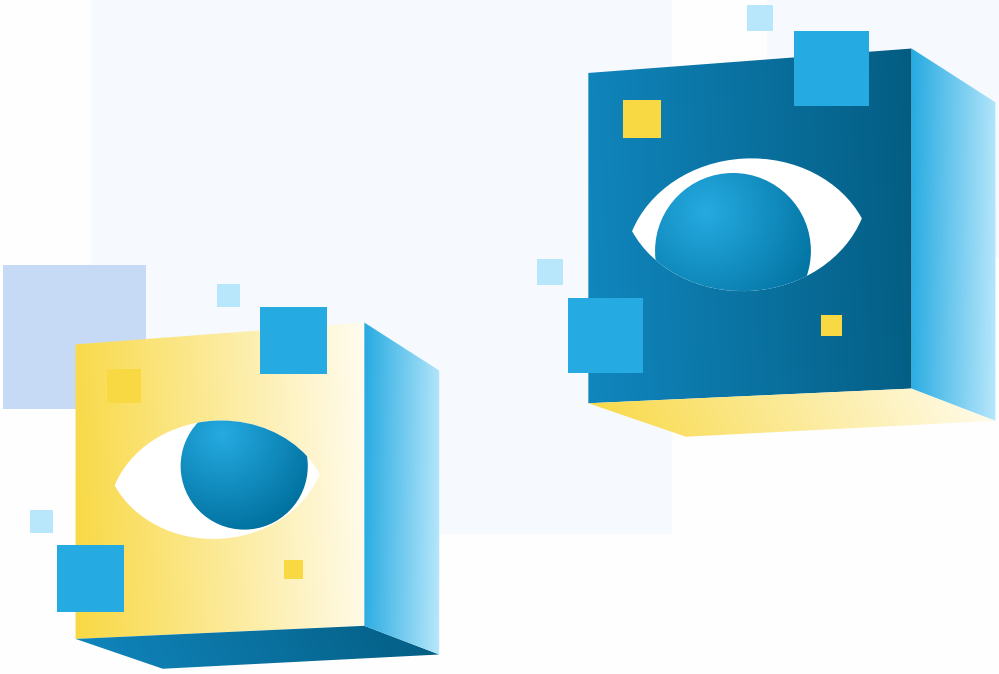
In the coming years, internet freedom strategies must adapt to Chinese users' online needs by providing accessible new pathways to information and facilitating otherwise censored interactions — a task that is far more complex than uncensoring websites or tunneling through firewalls. Peeling back the layers of China's information controls will require multiple actions across the public, private, and civil society sectors to advance a committed, positive vision of a global internet despite the realities of fracture and fragmentation.

> **If we do not attempt to contest China's model of internet substitution at its source, we will be unable to counter it where it spreads.**

Additional Resources

For a more detailed and comprehensive examination of threats to global internet freedom, please refer to Freedom House's latest edition of the annual Freedom on the Net report.





07 Project Highlights

China has undertaken a decades-long project to implement the most sophisticated information control system the world has ever seen, relying on multiple, overlapping, reinforcing mechanisms to prevent its population from experiencing the global internet. Authoritarian governments around the world are also learning from and ascribing to the PRC's draconian censorship and surveillance playbook, adopting its repressive technology to stifle free expression and political opposition.

While China has long been OTF's technical reference point for new technology development, OTF used FY 2024 funds to prioritize a series of targeted investments to better understand and more fully address elements of China's techno-totalitarianism. In addition to these, this section highlights projects which built resilience and responsiveness within censorship circumvention and privacy-enhancing technologies, and strengthened the digital security ecosystem.

During the reporting period, OTF supported over 43 innovative projects to circumvent censorship and enhance digital privacy and security; 11 cutting-edge information controls research efforts; and 15 rapid response interventions to address state-sponsored digital emergencies. In addition to direct financial support, OTF also offered services through revitalized Resource Labs to improve the security, usability, and accessibility of internet freedom tools — contributing to increased internet freedom technology adoption.

A full list of projects supported by FY 2024 funds is included at the end of this report.

Combatting the "Locknet"

China's approach to information control is not only the world's most technologically sophisticated, it is also the most expansive. The Chinese government is actively pioneering new models to perfect domestic control while shifting both norms and technical infrastructure abroad. OTF-funded research efforts supported by FY 2024 resources demonstrate the challenges posed by the breadth, depth, profusion, and ambition of the Chinese Communist Party's (CCP) efforts to reshape the flow of digital information both locally and globally.

In the first comprehensive technical analysis of China's censorship model, *The Locknet: How China Controls Its Internet and Why It Matters*, **ChinaFile's Jessica Batke and Northeastern University's Laura Edelson** showed that the widely held conceptualization of this system as merely a "Great Firewall" is outdated and incomplete. More than simply a "firewall," the CCP has been quietly erecting a "Locknet" — a multi-level, self-reinforcing system of socio-technical on- and offline controls. This system provides the Chinese government with unprecedented power to keep out foreign influence, and restrict and monitor what their population sees and says online. It does this while simultaneously facilitating China's global influence and commerce like any well-connected modern economy. The OTF-funded analysis also uncovered the mechanisms through which China implements this repressive control and how it is reshaping the internet's infrastructure in ways that affect users outside of China, too. This foundational research is crucial for developing innovative technical solutions that ensure independent information reaches individuals within China and countering the spread and normalization of this techno-authoritarian model. This report has redefined how policymakers and technologists understand the strategy that guides the implementation of Chinese information controls.

Chinese company Geedge Networks is exporting a censorship and surveillance product suite

that includes the ability to precisely identify and track users of VPNs and circumvention tools — even users who previously employed blocked VPNs.

Another pivotal research report, which received widespread media and stakeholder attention, uncovered how a Chinese company, Geedge Networks, is empowered by state norms to undermine free and open networks in a piecemeal fashion. OTF-supported digital forensics lab **InterSecLab**, and their partners, found that Geedge Networks is selling a comprehensive, turnkey censorship and surveillance system with China's Great Firewall capabilities to governments worldwide, including Ethiopia, Kazakhstan, Myanmar, and Pakistan. The findings reveal a fundamental shift: While authoritarian governments have historically spent years building patchwork surveillance systems, companies like Geedge are openly marketing comprehensive, enterprise-level product suites that provide any government client with instant access to cutting-edge tools (and dedicated customer support) for mass and precision surveillance and censorship. Geedge's product suite includes the ability to precisely identify and track users of VPNs and circumvention tools — even users who previously employed blocked VPNs.

Geedge and similar enterprises are "innovating to identify, block, and disable censorship circumvention tools while building resilience into their systems and making them sanction-proof through designed interoperability with most commercial network hardware providers." These capabilities underscore the ongoing challenge of maintaining online privacy and freedom of expression in the face of increasingly sophisticated censorship technologies, and raise numerous policy questions as more countries seek to simply import a commercial information control regime.

These research projects were foundational components of a broader OTF strategy to make iterative investments in a diverse range of privacy-preserving circumvention technologies that can begin to counter distinct layers of the Locknet. This is vital not only for users in China who are already deeply affected by the Locknet's information controls, but for those in countries whose leaders are learning strategic lessons from the CCP and importing technologies such as those provided by Geedge Networks.

Advancing Circumvention Technology

China's strategic innovations in information controls via the Locknet, and technological proliferation risk as demonstrated by Geedge Networks, add important new dimensions of authoritarian digital repression that require new approaches. At the same time, OTF's core focus areas, including advanced circumvention technologies, privacy-enhancing communications tools, and threat intelligence analysis and response capacity remain central in the struggle for internet freedom globally.

Surging Support for Circumvention Tools

As China, Iran, and other authoritarians invest in more sophisticated online information controls, demand for OTF-supported circumvention tools has increased by more than 500%. Through its Surge and Sustain Fund, OTF was able to support an unprecedented number of VPN users with FY 2024 funds — **over 45 million monthly active users in 18 countries on six circumvention tools.** OTF support for VPNs provides critical information lifelines to millions of people in digitally repressed environments who would otherwise be unable to securely access independent news and information. This investment contributed to increases in digital audiences for independent media operating in closed spaces, as well as an enhanced U.S. public diplomacy presence in these environments.

Demand for OTF-supported circumvention tools has increased by

more than 500%.

OTF supported an unprecedented

45 million monthly VPN users in 18 countries on six circumvention tools

with FY 2024 funds.

OTF's Surge and Sustain Fund is the first ever effort to consolidate U.S. government support for VPNs to maximize cost efficiencies, impact, and coordination across federal internet freedom funders. Through the Surge and Sustain Fund, OTF provides resources on a competitive basis to large-scale, open source circumvention tools with a documented track record of successfully circumventing authoritarian censorship in China, Cuba, Iran, Russia, and other closed information environments. The Fund covers the average per-user carrying costs for proven open source circumvention tools.

$0.07 per month (less than $1 per year)
cost to support one VPN user.

The tools funded under the Surge and Sustain Fund are selected through a public application process designed in conjunction with the State Department. This model ensures that the tools selected meet high security and privacy standards; and that they have a demonstrated ability to operate at scale in highly censored environments, with a track record of successfully staying ahead of increasingly sophisticated censorship techniques. Through the creation of this new mechanism, it now only costs on **average $0.07 per user per month — or less than $1 per year — to support a user on one of OTF's VPNs**.

Without OTF's support, users in highly censored countries like China, Cuba, and Iran would not have access to secure and effective circumvention tools at times when they need them most, particularly during periods of uncertainty and political crisis. In these moments, OTF's Surge and Sustain mechanism has proven to be both flexible and resilient. For example:

- **Iran:** After the anti-regime protests in Iran following Mahsa Amini's death, demand for OTF-supported VPNs skyrocketed. In response, OTF was able to quickly scale resources available for VPN users in Iran. At the protests' peak, **one in four Iranians** were relying on OTF-supported VPNs to access the uncensored internet.

- **China:** Over the last year, OTF was able to nearly double the number of VPN users in China to record levels as a result of continuous tool efficacy. This is all the more impressive given the CCP's meta-censorship of circumvention tools. OTF-supported VPNs were even directly targeted by the CCP last year, and they were able to adjust and counter these attacks, while their user bases increased.

- **Russia:** In Russia, demand for OTF-supported VPNs surged dramatically after the government began blocking YouTube. Simultaneously, the Kremlin targeted OTF-supported VPNs with attacks to take them offline. OTF-supported VPNs were able to weather these attacks while serving millions of new users.

While OTF was able to maximize resources available to support tens of millions of monthly VPN users, demand for these tools *continues to grow*. Authoritarians are evolving their information control playbook, and today, **nearly five billion people live in a country where the internet is censored**.

Developing Next-Generation Circumvention Tools

While OTF continues to invest in supporting tens of millions of circumvention users so they can access the uncensored internet, OTF also used FY 2024 resources to develop the **next generation of circumvention technology** to maintain a competitive advantage against quickly evolving authoritarian information controls. To ensure the resiliency and efficiency of these tools, OTF supported circumvention-detection advancements and the development of innovative technologies.

Circumvention tool developers previously thought that a diverse set of cover protocols could effectively overwhelm a resource-limited censor, preventing them from detecting and blocking all circumvention protocols at once through deep packet inspections. However, this approach was feeding an ongoing arms race between circumvention proxy developers, who implement obfuscation mechanisms to protect proxy traffic from detection, and censors seeking to penetrate these obfuscation layers. In response, OTF supported a comprehensive analysis into a novel strategy of **protocol-agnostic detection** in order to inform future technology development.

Many censorship circumvention and privacy-enhancing tools rely on injecting sensitive data into encrypted channels that leverage popular and proprietary network services. This has led to increased provider scrutiny, and even termination, limiting tool availability in repressive environments. In response, OTF supported the **SynthMorph** project to begin to develop a new circumvention tool that can bypass these network services by mimicking user interactions with them (e.g., videoconferencing). To date, they have successfully sent IP packets back and forth disguised as Web Real-Time Communication, which is a promising development for the viability of this next-generation technology.

Advancing Privacy-Enhancing Technology

Addressing network-level security vulnerabilities frequently exploited by authoritarian actors is crucial to protecting users accessing the free and open internet. OTF investments in this area improved the security of the internet as a whole, protecting billions of people from authoritarian surveillance and raising the cost of this repressive activity. These projects included new protections against Border Gateway Protocol (BGP) hijacking attacks that enable state actors to intercept HTTPS connections and surveil seemingly secure connections; as well as support for shorter-lived Transport Layer Security (TLS) certificates, which limit the opportunities to exploit compromised certificates. While not visible to end users, these and other infrastructural investments mitigate some of the most persistent and difficult-to-address security vulnerabilities for tens of millions of internet users in repressive environments.

A BGP hijack enables a repressive actor to pose as the legitimate owner of a foreign domain and obtain a trusted HTTPS certificate for that domain from a trusted certificate authority (CA). Having this HTTPS certificate allows the authoritarian censor to seamlessly intercept HTTPS connections, tricking the user into thinking they have a secure connection and allowing the malicious actor to steal sensitive information, like login credentials.

To address this, OTF supported the project **Fortifying Domain Validation**, which improved the domain control validation methods in order to make BGP hijacks much less likely to succeed; created new domain control validation methods that are immune to BGP hijack attacks; and developed better resiliency tools for CAs should they need to respond to attacks. Specifically, the project developed and deployed an effective countermeasure known as Multi-Perspective Issuance Corroboration, which was standardized at the CA/Browser Forum. This technology will soon be adopted by all CAs, marking a critical security milestone with outsized global impact.

Another ongoing project is drastically decreasing the risk of people who live under repressive regimes from visiting and engaging with compromised websites or IP addresses. Increasing **Internet Security Through Shorter-Lived TLS Certificates** is expanding the ability of Let's Encrypt, an automated CA, to issue TLS certificates with lifetimes of 10 days or less (it currently only offers 90-day certificates) for both Domain Name System-based (DNS-based) domains and IP addresses. Certificates with shortened lifetimes will mean that stolen keys and mis-issued certificates will be in circulation for a significantly shorter duration, greatly reducing the time that malicious actors who compromise website TLS certificates can monitor users.

Improving the Quality of Censorship Measurements

Quality censorship measurements are essential to understand and mitigate against the threats facing the free, open, global internet. The **Open Observatory of Network Interference (OONI)** and **Internet Outage Detection and Analysis (IODA)** projects are widely respected platforms providing visibility into internet shutdowns and other forms of repressive state censorship. With FY 2024 resources, OTF improved the security and reliability of these trusted platforms, so that there is greater transparency and understanding about authoritarian censorship trends.

OONI's censorship measurement and analysis relies on a global network of volunteers — many of whom are based in authoritarian information contexts — who run tests through OONI Probe to detect and document repressive internet censorship worldwide, increasing transparency about trends. As the OONI Probe network grows, so does the risk that some users (intentionally or unintentionally) taint measurements by supplying faulty data to the submission server. OTF support enabled OONI to create a probe-anonymous credential system that can provide verification at scale without de-anonymizing measurement contributors. The effort is improving the security and reliability of OONI measurements, and may be implemented into other open source internet freedom projects in the future.

OTF also invested in improving IODA, an internet monitoring platform that provides visibility into full connectivity shutdowns. In 2024, there were a historic 296 shutdowns across 54 countries, 47 of which continued into 2025. As the prevalence of these increased, OTF's FY 2024 investment contributed to IODA's reliability — extending coverage and increasing the accuracy of its measurements; providing users with greater context for disruptions by classifying autonomous systems; creating dashboard interfaces that provide intuitive measurement data that is actionable for both technical and less technical users; and providing curated data and tailored training and engagement that increased the use of IODA's data and platform. As of 2024, IODA has had over 17,000 users from 191 countries.

Strengthening Local and Regional Digital Threat Intelligence

Readily available commercial spyware has made it faster and easier for governments to target their citizens, regardless of their physical location. Journalists and civil society leaders are often the first targeted and the ones least likely to have the resources to push back.

In many local contexts, there are few civil society organizations working to identify and mitigate digital threats. Those that do, often work in isolation, and few have the expertise or resources to keep up with the pace or sophistication of new state-sponsored surveillance threats. The lack of coordination among these organizations, combined with significant research gaps, means they often miss critical vulnerabilities.

OTF investments are maximizing the impact of digital security help lines

to keep pace with authoritarian tactics and better protect civil society members most vulnerable to novel attacks.

With FY 2024 funds, OTF worked to strengthen the ecosystem of threat intelligence analysis and response through continued investments in sustainability and threat intelligence-sharing efforts across regional help desks. These investments are maximizing the impact of digital security help lines to keep pace with authoritarian tactics and better protect civil society members most vulnerable to novel attacks.

Following previous investments that supported threat intelligence sharing across regional help desks in the Eurasian region, Iran, and Ukraine, OTF expanded these to include other regions where civil society has historically been heavily targeted by authoritarian actors. For example, **Terali** is technically integrating digital security help desks in East and Southeast Asia into a wider network that maps and identifies digital attack trends, shares threat intelligence, and coordinates warning systems. As a result, civil society organizations in Cambodia, Hong Kong, Tibet, and Vietnam, who are particularly vulnerable to digital security attacks, can more readily report incidents, request assistance, and understand the holistic nature of the threats they face.

In addition, OTF supported the **Center for Digital Resilience** to strengthen and expand the number of expert-level digital security providers, particularly in critical areas such as threat research and digital forensics, in order to better meet growing demand in authoritarian and emerging authoritarian information contexts. This resulted in an increase in the quality and availability of technical assistance accessible to communities in need.

Responding to Digital Emergencies

Over the course of 2025, the frequency, volume, and sophistication of authoritarian state-sponsored cyber attacks have increased significantly around the world. OTF received more than 300 applications for emergency assistance through its Rapid Response Fund, an increase of 70 percent over the previous year.

70% increase

in demand for emergency, digital security assistance.

Notable among these, OTF helped civil society organizations supporting the resettlement and safety of North Korean refugees, who had been targeted repeatedly by the North Korean regime. These organizations received emergency, digital security audits in order to help them protect their data. The effort uncovered several vulnerabilities and attacks, including critical web application flaws and sophisticated, multi-wave phishing campaigns. Auditors then helped these organizations harden their digital infrastructure and protocols to better protect against future attacks.

The Rapid Response Fund also helped independent media organizations, particularly in Russia, get back online after sudden censorship events and strengthen their digital security. This included investigating denial-of-service-attacks, developing mitigation strategies, and improving website security.

Innovative Information Controls Research

OTF supports technical, leading-edge research to fully understand emerging authoritarian censorship and surveillance tactics in order to cost-efficiently contribute to the technology development cycle. Last year, researchers detailed nascent regional censorship trends, the use of generative AI for information controls, and the growing proliferation and sophistication of repressive surveillance technologies.

One project identified specific implementations of censorship in five LLM services hosted in China, and then developed circumvention methods to bypass them.

In 2025, much of OTF's research focus complemented a broader strategy to develop circumvention solutions that counter the CCP's "Locknet" within China and its wider sphere of influence. For example, one project researched how China is extending information controls to generative AI (GenAI) tools. GenAI technologies, such as image and video generation and sophisticated chatbots, are significantly lowering the barriers to creating convincing digital content. In authoritarian nation-states with stringent information controls, such as China, monitoring and deploying Large Language Models (LLMs) poses a compliance challenge to service providers, as they are beholden to a rigid set of communication and information directives. The project identified specific implementations of censorship in five LLM services hosted in China, and then developed circumvention methods to bypass them.

As the proliferation and sophistication of repressive surveillance technologies intensifies, OTF also invested in research projects to uncover their scale and technical capabilities. One project investigated the digital threat landscape in South America — mapping spyware methods, the intricate connections between surveillance companies, and their funding sources and affiliations. The project, which disseminated findings via a Surveillance Watch website, helped civil society protect their privacy by improving understanding of the threat landscape. The methodology developed in this research will also be applicable and useful for other geographic contexts prone to authoritarian surveillance.

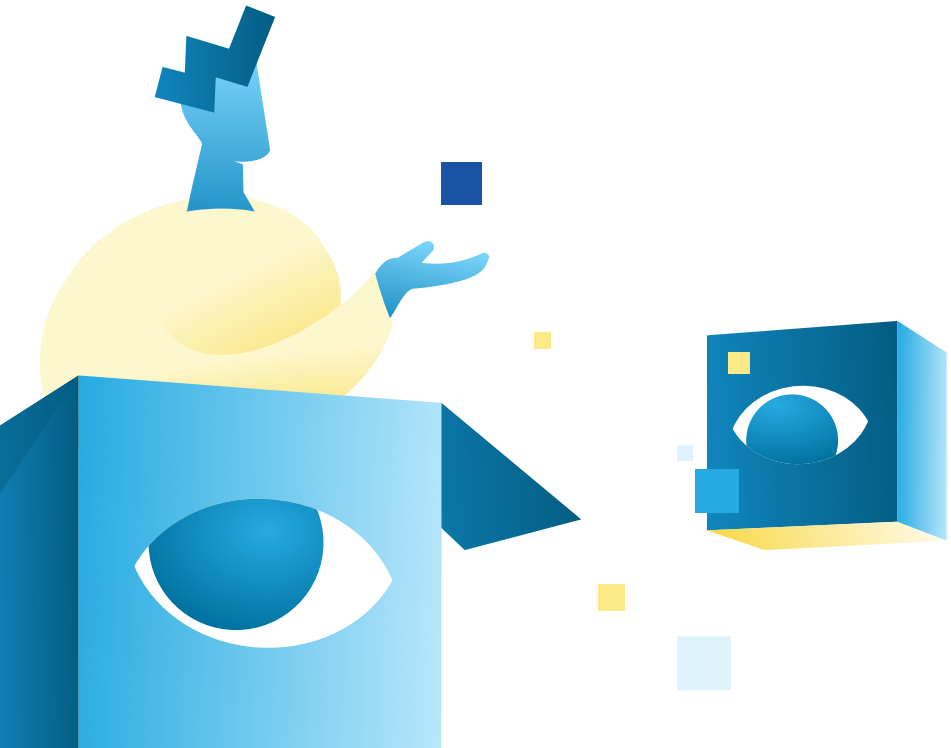
Similarly, OTF supported research into the technical makeup, capabilities, and infection vectors of a novel form of spyware. The project uncovered how the tool exploits vulnerabilities in the Android system and is engineered for sustained data harvesting. Its alarming capabilities include interception and redirection of SMS messages in real time, extraction of call history, and continuous audio recording and location tracking. The findings reveal vulnerabilities within Android's security architecture that facilitate such pervasive surveillance in authoritarian contexts.

Revitalizing OTF's Resource Labs

OTF provides expert services to support internet freedom technologies and researchers through its Resource Labs: the Security Lab, the User Experience & Discovery Lab, and the Impact & Engagement Lab. The services provided ensure that the technologies OTF funds are secure, accessible, and widely adopted by users in repressive environments. The Lab model also helps OTF achieve economies of scale and cost efficiency. Following the successful redesign of the Security Lab with FY 2023 resources, OTF's FY 2024 resources were used to revitalize additional Labs, refining their scope and updating the services provided to more accurately reflect projects' needs and their impacts.

For example, the **User Experience & Discovery (UXD) Lab** — formerly the Secure Usability & Accessibility Lab — supports projects with their usability and accessibility design needs. FY 2024 funds enabled OTF to expand the number of service providers and offerings to include user-centered research and other discovery services, helping technical projects better understand who their users are, and what they need from internet freedom technologies.

OTF also revamped support for audience engagement and end-use of internet freedom tools through a greater diversification of vendors and services under the **Impact & Engagement Lab** (formerly the Learning Lab). This effort helped projects more effectively communicate their overall impact in support of establishing efficacy and security, building community trust, increasing engagement with their work, and sharing innovation.



08 Supported Projects

Surge and Sustain Fund

Anti-censorship tools have become a prerequisite for billions of people around the world to access the free and open internet. OTF's Surge and Sustain Fund supports the per user costs of leading circumvention tools — at less than one dollar per year per user — to enable tens of millions of people living in highly censored countries to access the uncensored, global internet.

Psiphon

$9,064,132

Psiphon Inc.

Psiphon is one of the most technically advanced and widely used circumvention tools in the world, helping tens of millions of people to overcome censorship and connect to the uncensored internet. Support from OTF enabled Psiphon to provide services to millions of monthly users in Cuba, Iran, Myanmar, Russia, and other authoritarian contexts.

---

nthLink

$3,931,548

Advanced Circuiting Inc.

nthLink is a powerful anti-censorship application capable of circumventing internet censorship and self-recovering from blocking events. Support from OTF enabled nthLink to provide services to millions of monthly users in China, Iran, and Russia, and significantly grow their user base in these countries.

VPN Provider

$594,454

Cyber security experts

This project helped users in Iran and other authoritarian contexts access the open internet. OTF support enabled the tool to serve millions of people experiencing repressive censorship.

Lantern

$480,567

Brave New Software Project, Inc.

Lantern is a free peer-to-peer internet censorship circumvention tool that delivers fast, reliable, and secure access to the open internet. Support from OTF enabled Lantern to provide services to users in China, Iran, Myanmar, and Russia.

Rostam VPN

$307,122

U.S.-based network & cybersecurity experts

Rostam VPN is an established and reliable censorship circumvention tool that supports millions of monthly users in Iran. The application relies on the open source WireGuard protocol, which has a lean codebase — allowing faster connection times and more responsive performance, even on networks with high latency. With the support of OTF, the tool grew its user base in Iran.

FreeBrowser

$41,584

GreatFire

FreeBrowser is a censorship-resistant web browser that provides uncensored access to the open internet. The open source tool works like a normal web browser, but allows users to load websites that have been blocked by authoritarian censors. OTF support enabled the tool to serve a significantly increased number of users in China, Iran, and Turkmenistan.

Internet Freedom Fund

The Internet Freedom Fund (IFF) is the principal mechanism through which OTF supports innovative internet freedom projects. IFF projects primarily focus on technology development and implementation, but also include applied research and digital security efforts. OTF solicits IFF project proposals on a rolling basis through a fully open, transparent, and competitive process.

Developing Innovative Circumvention Solutions

Increasing Internet Security

$800,000

Internet Security Research Group

TLS certificates authenticate a website's identity and enable encrypted communication between a browser and server. They secure data in transit and verify that a website is not a fraudulent imposter. Compromised certificates enable malicious actors, such as authoritarian censors, to monitor internet users and block access to information. Internet Security Research Group's nonprofit certificate authority (CA), Let's Encrypt, is the world's largest CA, currently used by over 700 million websites to encrypt their traffic using free, automated TLS certificates. OTF supported shortening the lifespan of TLS certificates from the current default time of 90 days to 10 days. Certificates with shortened lifetimes means that stolen TLS keys and mis-issued certificates will be in circulation for a shorter period of time. This will drastically decrease the risk for people who live under repressive regimes visiting and engaging with websites or IP addresses that have been compromised. Further, it will greatly reduce the timespan in which authoritarian censors who compromise website TLS certificates can monitor citizens.

Fortifying Domain Validation

$585,740

Princeton University

Border Gateway Protocol (BGP) hijacking is a common technique that repressive censors use to monitor and intercept digital communications. Through a BGP attack, authoritarians pose as the legitimate owner of a foreign domain and allow it to obtain a trusted HTTPS certificate for that domain from a trusted Certificate Authority (CA). Having this HTTPS certificate allows the censor to seamlessly intercept HTTPS connections, fooling the victim (e.g., a citizen) into establishing an encrypted connection with the adversary (e.g., the repressive regime) instead of the victim's intended destination.

This project presented the first analysis framework for measuring the security of Multi-Perspective Issuance Corroboration (MPIC), an emerging defense for mitigating BGP hijacks. As a result of this effort, the CA/Browser Forum unanimously adopted MPIC as a standard. All CAs will be adopting this MPIC technology, which will help protect users' privacy in repressive information contexts.

Robust Multi-Protocol Tunneling

$492,941

INVISV

Internet privacy and circumvention technologies often depend on tunneling protocols to prevent traffic from being blocked or altered. These protocols, however, often use non-standard transport methods that make their traffic identifiable, and thus subject to blocking. This project developed PseudoTCP stack for INVISV MASQUE, an open source implementation of the Internet Engineering Task Force standard MASQUE, that makes circumvention traffic harder for censors to identify. The MASQUE protocol enables Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) traffic to tunnel through web servers using HTTPS so that data sent via a MASQUE tunnel will appear to be HTTPS traffic from the network's standpoint. PseudoTCP stack will enable the development of MASQUE-based Android VPNs and video conferencing — helping people in repressive contexts access the open internet and securely communicate.

Investigating Protocol-Agnostic Methods to Fingerprint Obfuscated Circumvention Traffic

$313,164

Armin Huremagic & Regents of the University of Michigan

Until recently, there was a consensus that a diverse set of cover circumvention protocols can effectively overwhelm a resource-limited authoritarian censor, preventing them from detecting and blocking all censorship circumvention protocols en masse. However, in 2022, Chinese censors aggressively blocked various Transport Layer Security-based (TLS) circumvention tools, suggesting they detected TLS-based proxies using a novel approach: "TLS-in-TLS." Instead of targeting specific circumvention tools, the approach focused on the unusual pattern of nesting one TLS layer within another — a behavior shared among TLS-based proxies but rare in standard web browsing. To address this emerging threat, this ongoing project is conducting a comprehensive analysis of the risks of censors detecting and disrupting circumvention-tool usage by targeting encapsulated layers within the cover circumvention protocols (as opposed to the cover protocols themselves). The goal is to help developers strengthen circumvention technologies against this type of detection in order to improve those technologies' resilience for users in authoritarian contexts.

The Geopolitics of Communication Infrastructure

$303,514

University of Amsterdam

While there is much research into the technical workings of censorship regimes in China and Russia, there is a lack of investigation into the political and technical processes and policies that shape their information networks and controls. To fill this gap, this ongoing project is conducting an in-depth analysis of Chinese and Russian technology infrastructure policies. The effort will deepen our understanding of how these infrastructures are evolving and shaping information control measures. The project also aims to uncover the policy-implementation pipeline, including which actors are involved, and investigating how these dynamics impact the way censorship circumvention tools work.

WeiboCensor Insight NLP Powered Analysis

$103,305

The Board of Trustees of the University of Illinois

Weibo, often referred to as "China's Twitter," is a primary platform for public discourse in China. The Chinese government employs advanced AI algorithms on Weibo to control what users see and discuss. While earlier research has mostly focused on the deletion of posts, recent trends show that content understanding-based censorship — where posts remain visible but with limited interactions or are selectively shown — is becoming more prevalent. Using machine learning and AI algorithms, these systems analyze content across multiple factors — such as context, topics, sentiment polarity, user influence, and language patterns — to determine whether to restrict the content. This ongoing project will identify common patterns in censored content to understand how AI-driven censorship systems operate, and provide valuable insights for counter-censorship efforts. The project webpage includes an overview of the research, preliminary findings, and visualizations summarizing results to date.

SynthMorph

$74,207

University of Waterloo

Many anti-censorship and privacy-enhancing tools leverage popular and proprietary network services. However, some companies have taken issue with the use of their infrastructure for censorship circumvention, further restricting the availability of internet freedom tools for people in information repressive contexts. To address this challenge, the SynthMorph project is developing a censorship-resistant tool that mimics user interactions with service providers like videoconferencing applications — bypassing the need for providers' approval.

With OTF support, the unique tool is using machine learning techniques to synthesize traffic that inconspicuously carries data repressive censors might find objectionable, enabling users to access the free internet while avoiding detection. This project will also develop a user-facing prototype.

Enhancing Secure Communication Technologies

Shout SMS

$899,981

Gisa Inc.

Encrypted shutdown-resilient communications are critical for securely reporting on and staying connected during authoritarian internet shutdowns. Shout SMS is an ongoing project working to provide civil society and journalists in shutdown-prone contexts with a new, secure, SMS messaging tool. The tool enables private communication of text and images even when the internet is slowed, unreliable, compromised, or shutdown altogether. With OTF support, the Shout SMS team carried out initial technical research, and completed early-stage technical development.

Session Activist Enhancements

$339,829

OPTF Ltd.

Session is a peer-to-peer secure messaging application that emphasizes user anonymity and confidentiality. At-risk communities in repressive contexts often rely on this tool, especially when other mainstream messengers like WhatsApp and Signal are censored. With OTF support, this project developed features to enhance the application's safety, security, and censorship circumvention capabilities.

dComms

$47,038

eQualit.ie

Authoritarian governments are increasingly turning to widespread network shutdowns to prevent all methods of circumventing their repressive censorship. In addition, they are replacing international platforms, such as WhatsApp, with local, government-controlled alternatives which often contain privacy and security vulnerabilities. These leave populations without secure, reliable options for accessing and sharing information, or communicating with each other. This project developed and deployed decentralized communications (dComms) infrastructure in five shutdown-prone countries. The goal was to better understand how populations in these contexts can leverage federated networks to communicate resiliently and securely.

Partisan Telegram for Android

$32,846

Fundacja Bialorus Liberty

Telegram Messenger is a popular communications platform in a number of authoritarian contexts, such as Belarus and Russia. However, compared to more purpose-built secure messaging applications, it offers little privacy or data protection for users. To address this problem, Partisan Telegram is an interoperable modification of the app that contains extra data protection features to keep users in repressive information environments safe. This project developed new privacy features to further enhance user security from authoritarian surveillance.

Improving Censorship Measurements

IODA: Observatory for Real-Time Monitoring and Analysis of Internet Blackouts Caused by Censorship

$608,849

Georgia Tech Research Corporation

The Internet Outage Detection and Analysis (IODA) project is a free, open source internet monitoring platform that provides visibility into full connectivity shutdowns. It enables users to investigate disruptive events and provides tool developers with data to analyze the events and improve censorship circumvention technologies. With OTF support, IODA improved its reliability as a global, public service. It did this by extending its coverage and accuracy of measurements; providing users with greater context for disruptions by classifying Autonomous Systems; creating dashboard interfaces that provide intuitive measurement data that is actionable for less technical and technical users; and providing curated data and tailored training that increases IODA's use within the internet freedom community.

Developing Test Lists for Censored Online Content

$360,529

Netalitica Inc.

Probing for blocked online content is a key component of projects assessing the state of information controls in censorship hotspots around the world. While network probes used for this purpose have greatly evolved over the years, the URL databases (i.e., Citizen Lab test lists on GitHub) that the probes draw upon have not. This negatively affects the quality of collected measurements. This ongoing project is updating the test lists of 60 countries. It is also improving the methodology of test-list updates, and collaborating with research organizations to automate aspects of the test-list update process. These efforts will increase the quality of collected measurements, and enable researchers to produce reports that accurately portray repressive internet censorship on the ground.

OONI Anonymous Credentials

$289,341

Open Observatory of Network Interference

The Open Observatory of Network Interference (OONI) provides free, open source software for measuring internet censorship and other forms of network interference around the world. They also publish censorship measurements that are crowdsourced by users worldwide, many of whom are based in repressive contexts. In response to increased threats from the Chinese government and other authoritarian regimes, this project is supporting the creation of a probe-anonymous credential system to help identify and remove faulty measurements while protecting user privacy. This ongoing project will not only improve the security and reliability of OONI measurements, but will also improve the measurements of other crowd-sourced open source projects by providing them with access to the new credentialing system.

IRBlock: A Large-Scale Measurement Study of the Great Firewall of Iran

$150,000

The University of British Columbia

Iran's national filtering system, an important part of its online censorship regime, employs multiple layers of interference across several core internet protocols; and its behavior has evolved quickly over time. Yet, systematic, comprehensive measurement of this system remains difficult because reliable in-country vantage points are hard to obtain and maintain. IRBlock, a large-scale, longitudinal censorship measurement system focused on Iran, will address this gap by developing and operating a scalable measurement system to continuously map censorship behavior at-scale and track changes over time. This project will include updated datasets, technical analysis, and public reporting, which will provide evidence-based visibility into what content is blocked and how filtering is implemented. This will contribute to more robust circumvention strategies.

Strengthening Local and Regional Digital Threat Intelligence

HIVE: The CDR Program for Digital Security Service Providers

$996,606

Center for Digital Resilience Ltd.

Many civil society organizations lack the expertise or resources to keep up with the pace or sophistication of new state-sponsored surveillance methods and other digital threats. To strengthen the digital security ecosystem, the Center for Digital Resilience's HIVE Incubator Program provided 20 mid-level digital security practitioners with advanced training in a number of relevant domains. These included advanced phishing tactics, server administration, forensic analysis, malware analysis, vulnerability assessments, and penetration testing.

In addition to the technical substance of the program, trainees also learned best practices for engaging civil society organizations prone to repressive censorship and surveillance through an organizational security audit, conducting proper digital threat mapping, and sharing threats and vulnerabilities with individuals at a global scale in relevant, contextual, and safe ways. By training and mentoring mid-level digital security providers, particularly in critical areas like threat research and digital forensics, the program enhanced the resilience of at-risk communities against escalating digital attacks, enabling sustained support and fostering an independent ecosystem of digital resilience.

Terali: East & Southeast Asia Civil Society Resilience

$971,763

Center for Digital Resilience Ltd.

Civil society in East and Southeast Asia are increasingly targeted by state-sponsored digital attacks, yet the majority of these actors lack the resources or capacity to protect themselves. The small number of organizations that do have the resources rarely share threat intelligence data, which could help others facing similar attacks. This ongoing project will improve the security of civil society in the region through the adoption of a widely used threat analysis platform and ticketing system that coordinates the work of digital security help desks and alert networks globally. These networks are critical for mapping and identifying digital attack trends, sharing threat intelligence, and coordinating warning systems. As the procurement of dangerous spyware is spreading among authoritarian governments, this initiative is crucial for the security of individuals in information repressive contexts.

Digital Support Help Desk

$438,375

Digital security experts

This project established a help desk to support people experiencing state-sponsored digital threats. It also created a robust network and knowledge base, contributing to threat intelligence coordination efforts that enhanced the resilience and security of civil society in repressive information contexts.

InterSecLab Phase 2

$435,874

Brava Tech Def Ltda.

InterSecLab is a digital forensics laboratory that works with civil society organizations to monitor and map threats to users facing repressive censorship and surveillance. While OTF previously supported the Lab's establishment, this project focused on critical infrastructure updates and digital forensics work with global implications.

Notably, InterSecLab provided technical analysis of a massive data leak that exposed how Chinese company Geedge Networks deploys powerful censorship and surveillance technologies across multiple countries, including Ethiopia, Kazakhstan, Myanmar, and Pakistan, as well as within China's own provinces. The report, *The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting the Great Firewall to Autocratic Regimes*, reveals a suite of repressive products — including deep-packet inspection to intercept and manipulate user traffic and malware infection — and illustrates how their export is fundamentally transforming how quickly and easily authoritarians can control digital communications.

Strengthening the Digital Security Ecosystem in Central Asia

$322,710

National Legal Corporation

As part of OTF's threat intelligence coordination efforts, this project established a help desk for civil society in Central Asia, specifically supporting independent media and civil society organizations in Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan who face increasingly complex digital threats and transnational repression. The project established a coordinated regional network of cybersecurity experts to conduct cybersecurity monitoring, research, and analysis of cyberattacks targeting civil society in the region. The network also provided early notification of cybersecurity vulnerabilities and risk mitigations to organizations, as well as rapid response remediation to those targeted.

PiRogue Tool Suite (PTS) 2

$240,205

Defensive Lab Agency

Many digital forensics tools are closed source, complex, and costly. The PiRogue Tool Suite (PTS) is an open source, user-friendly, and free digital forensic analysis and incident response solution. It is an accessible option for resource-contrained and non-technical civil society members who are often the main targets of repressive censorship and surveillance. This project supported the development of PiRogue VPN, which enables civil society organizations to perform forensic analysis without the need to invest in their own hardware. The application has recently been used to analyze and map a particular set of browser-based geolocation phishing attacks. The project also improved its knowledge management component Colander, enhanced interoperability with other threat intelligence platforms, and developed offline artifact analysis — enabling the local analysis of files without relying on third-party services, and therefore increasing case confidentiality.

Strengthening Digital Security for Journalists

$154,619

Human Rights Network for Journalists-Uganda

The Ugandan government often censors the internet to control the flow of information and curb the spread of dissenting views or opposition narratives in the country. This censorship limits the ability of journalists to report on sensitive issues and hold those in power accountable, stifling media freedom and the dissemination of objective views. In this climate, cyber attacks against journalists have become prevalent, including the hacking of devices and social media accounts, data theft, and surveillance through malware and spyware. This project helped 15 media organizations in the country improve their digital security posture by creating security policies and incident response procedures. It also developed a digital security handbook that provides journalists with comprehensive and accessible information about context-specific threats.

Strengthening of Digital Security of Southern Africa / ConnectCon 2024

$131,804

Digital Society of Africa

ConnectCon is an annual convening for digital security practitioners based in Southern Africa, and is an important space for circumvention technologists to receive feedback from digital security practitioners in the region. OTF supported sessions to train digital security providers on circumvention and privacy-enhancing tools as part of a focus on improving threat intelligence collection and sharing. Feedback from these sessions has been used by developers to improve usability and functionality of critical internet freedom technologies.

Strengthening the Internet Freedom Ecosystem

Global Voices Summit 2024

$209,869

Stichting Global Voices

The Global Voices Summits are critical spaces for civil society to gain digital security knowledge and skills, increasing their resilience against authoritarian censorship and surveillance. OTF supported the digital security track at the 2024 Summit, which had approximately 300 participants. The knowledge participants gained from this track informed the work of the Global Support Link, a collective of security practitioners collaborating on the OTF-supported help desk CDR Link — a secure platform for aggregating, displaying, and sharing data on digital security threats and attacks facing civil society globally.

Forum on Internet Freedom in Africa 2024

$90,087

Collaboration on International ICT Policy for East and Southern Africa

Forum on Internet Freedom in Africa (FIFA) is one of the leading internet freedom convenings bringing together technologists and researchers. This project supported FIFA's digital security track, including a dedicated digital security help desk for civil society attendees who are vulnerable to digital attacks.

Rapid Response Fund

The Rapid Response Fund provides emergency support in response to state-sponsored digital attacks. Support obtained through this fund helped those targeted regain online access, mitigate future attacks, and combat sudden censorship events.

Localization Lab

$216,310

Localization Lab

Localization Lab is a nonprofit that engages in rapid interventions to translate critical censorship circumvention and privacy-enhancing resources into numerous languages — ensuring that internet freedom tools are accessible and comprehensible to the users during times of crisis.

Security Matters Asia

$129,000

SECM Tech Solutions

Security Matters Asia (SecM) is a nonprofit group empowering civil society in Asia to stay safe and resilient. Their services include localization (ensuring internet freedom tools resonate in a specific region or country), organizational security, and digital security assistance. With OTF support, SecM improved the resilience of several independent media outlets after multiple state-sponsored cyberattacks. This involved addressing critical vulnerabilities in outlets focused on Cambodia, Hong Kong, and North Korea that needed to safeguard their operations and the integrity of their content quickly. SecM's work with these outlets included developing organizational digital security policies, conducting tailored staff trainings, and developing incident response plans.

InfosecLabs

$110,000

InfosecLabs LLC

InfosecLabs is a collective of technologists committed to strengthening the information security of civil society in Latin America. Their services include organizational security and digital security support, as well as digital attacks response and forensic analysis. With OTF support, InfosecLabs helped civil society actors and journalists targeted by state-sponsored digital attacks through comprehensive risk assessments and tailored digital security trainings.

eQualitie

$100,000

eQualit.ie

eQualitie develops circumvention technologies for use in contexts where the internet is being repressed. They provide remediation in response to digital attacks, forensic analysis, and secure web hosting. With OTF support, they helped civil society organizations from El Salvador, Nicaragua, Russia, and Ukraine, among other countries, respond to sudden censorship events.

VPN Generator: Circumventing the Russian YouTube Blockade

$52,305

IEDN

VPN Generator is a popular VPN service provider in Russia. When Russian authorities throttled and functionally blocked YouTube — the last remaining uncensored platform in the country — VPN Generator was able to provide access to more than 200,000 unique users.

Defend Defenders

$50,000

Defend Defenders

Defend Defenders operates a digital security help desk that supports civil society in Eastern Africa who are facing state-sponsored digital emergencies. Their services include organizational security and digital security support, and urgent risk mitigation. With OTF support, they helped civil society organizations in Ethiopia, Kenya, Tanzania, Uganda, and Zambia harden their organizational digital security posture post-emergency.

Meduza

$49,992

Medusa Project LLC

Meduza is a Russian-language independent media outlet with a significant audience in Russia, serving as a critical source of information for millions of people subject to Kremlin censorship. After Meduza managed to overcome an intense state-backed cyberattack, OTF support helped the outlet improve their website security to be more resilient to future attacks.

Internet Freedom Technical Upskilling

$49,988

Digital Security Expert

The political climate in Tanzania has become increasingly authoritarian, with the government imposing platform blocking, a ban on VPNs, and internet shutdowns. As the 2025 national elections neared, the threat of more shutdowns loomed large and the need for effective circumvention solutions was urgent. This rapid response project adapted and tested the "Go Bag Toolkits" (a kit of shutdown resilience tools) user research and training methodology to understand the resilience needs of ten Tanzanian civil society organizations. The project also provided valuable feedback on the usability and efficacy of shutdown resilient tools, highlighting further directions for technology design and implementation.

Secure Technological Infrastructure for ACHR

$49,891

Centre d'accès pour les droits de l'homme (ACHR)

ACHR is a refugee-led organization that uses open source tools to document human rights violations. Because of the sensitivity of their work, ACHR has experienced multiple digital security incidents attributed to state actors in repressive environments. The project strengthened the security of their technological infrastructure and enabled them to establish a minimum viable digital security baseline in order to continue their work.

---

eSIM Connectivity Fund

$49,400

Digital Security Experts

One of the many negative consequences of internet shutdowns is the loss of vital communication services, preventing people from connecting with emergency services and loved ones. Innovative methods to restore connectivity are essential. The eSIM Connectivity Fund project focused on researching solutions and developing a methodology to effectively distribute over 29,000 embedded SIMs (eSIMs) to civil society and journalists in conflict areas where internet connectivity is limited. These eSIMs, from telecommunications providers in non-repressive contexts, connect users to remote networks — allowing them to circumvent connectivity blackouts in their region.

Improving Secure Documentation Tool Tella

$43,384

Horizontal

Tella is a mobile tool that makes it easier and safer to document human rights violations and collect data in authoritarian contexts. OTF is supporting the tool to make technical improvements to its digital safety protection and file sharing features before deployment in high-risk contexts. This will enable users to protect themselves from repressive surveillance and safely document state-sponsored repression. The project is also implementing recommendations from a recent security audit to ensure it is as secure as possible for users, as well as providing an instance of the tool on a virtual private server — a type of hosting that provides better stability, performance, and security than shared hosting.

Na Svyazi

$41,010

Fundacja Stay Connected

Na Svyazi is a nonprofit organization that provides digital security support and monitors internet freedom in Russia. OTF supported the maintenance of their RuNet Monitor, a web platform for collecting and analyzing network outage information in Russia. As the Russian government significantly increased online censorship in 2025 — throttling YouTube and shutting off entire regions from the global internet — maintaining and improving RuNet was critical to accurately track this escalation in information controls. The project improved the platform's visualizations and developed a collaboration tool prototype for their volunteers who report network disruptions and outages.

Qurium Media Foundation

$21,000

Qurium Media Foundation

Qurium Media Foundation (QMF) helps remediate digital threats and emergencies in a timely and comprehensive manner. Their services include organizational security and digital security support, digital attack response and forensic analysis, secure web hosting, and connectivity-issue remediation. With OTF support, QMF helped an independent media outlet in Georgia when they suffered severe data security threats after reporting on pro-Russian activities in the country.

Securing Digital Spaces Senegal

$20,562

Polaris Association

In Senegal, there is an ongoing need for strong digital security measures to protect civil society. Given a history of internet freedom challenges during electoral periods, Polaris, a civic tech nonprofit organization, provided digital security support to 40 civil society members in three cities in the lead up to the country's general elections. They also set up a PiGuard WiFi router so journalists could securely access the open internet.

Response to Cuban State Censorship of Independent Media Outlet

$14,001

Mas Voces Foundation Inc.

An independent Cuban digital media outlet experienced a large-scale DDoS attack, along with state-imposed blocking of its website and related infrastructure in December 2025. Without urgent technical intervention, the outlet faces continued service disruption and the risk of prolonged information blackouts affecting their users. This project will incorporate a VPN layer within the outlet's apps so that it can function during blocking, traffic filtering, or network interference. This approach enables users to maintain access without requiring manual configuration or external tools, reducing service disruption during censorship events.

VOD Digital Security Incident Response

$10,139

Foundation For Freedom

Voice of Democracy (VOD) is one of the few remaining independent media outlets in Cambodia. It has faced increasing threats to its digital security since the government revoked its media permit in 2023. With OTF support, VOD identified digital security priorities and engaged with Security Matters Asia (a digital security organization and one of OTF's Rapid Response Fund vendors) to harden its security posture.

Free and Open Source Software (FOSS) Sustainability Fund

Many open source technologies are the foundation of the free and open internet. Yet despite the critical role they play in protecting free expression, these resources are perpetually underfunded and undersupported, which creates security vulnerabilities. The FOSS Sustainability Fund ensures free and open source software projects — and the communities that sustain them — have the resources and support needed for long-term maintenance.

Tails Sustainability

$382,310

Tor Project

Tails is a portable operating system that protects against authoritarian censorship and surveillance. This project supported essential day-to-day maintenance, upgrades, and improvements, including resolving long-standing usability issues. OTF funding also supported long-term sustainability, enabling, among other things, enhanced fundraising capacity.

F-Droid Sustainability

$371,974

Hans-Christoph Steiner

F-Droid is a globally trusted Android app store, which enables users in repressive internet contexts to download secure communication and circumvention tools where they are often inaccessible via other app stores. OTF is supporting critical maintenance activities, including automating localization activities; standardizing informed responses to government app takedown requests; and streamlining the management, custody, and control of funding for long-term project sustainability.

Reproducible Builds Sustainability

$301,290

Software Freedom Conservancy, Inc.

Reproducible Builds is a set of software development practices that create an independently verifiable path from source to binary code. These practices allow users to verify that vulnerabilities have not been introduced, and ensure supply chain security and integrity, which is critical for internet freedom tools.

Funding from OTF for this project supported building the reproducibility of software packages, and helped provide technical improvements and day-to-day maintenance support for tools. During the project, contributors fixed over 437 unreproducible packages, and sent these patches upstream to the corresponding platform/language ecosystem. The project also improved documentation, grew the developer ecosystem, and lowered the bar for entry for new contributors — supporting the project's overall long-term sustainability.

Mailvelope Sustainability

$250,000

Mailvelope GmbH

Mailvelope is an established, open source secure communication tool that provides end-to-end encrypted email. This project supported ongoing software development, maintenance, and usability improvements. Support from OTF also helped Mailvelope improve their financial sustainability by growing the commercial "Mailvelope for Business" branch. This included signing a partnership with Nextcloud to offer Mailvelope services.

Improving the Sustainability of the OONI Software Ecosystem

$243,535

Open Observatory of Network Interference

The Open Observatory of Network Interference (OONI) is a real-time censorship measurement platform that monitors censorship in over 200 countries worldwide. Since its inception in 2012, OONI has collected more than one billion network measurements from 241 countries, and published 85 research reports documenting internet censorship around the world. They were the first to detect novel internet censorship events in Cuba in 2019, and in Kazakhstan in 2022, among others. The OONI software ecosystem requires ongoing maintenance to ensure that real-time internet censorship data is collected and published reliably, securely, and at scale. Support from OTF for this project helped conduct infrastructure maintenance and improve a host of components, including code and data quality, dependency updates, refactoring code, usability, and documentation.

Transition Tor Browser to Firefox ESR 14

$202,213

Tor Project

The Tor Browser is a widely adopted, user-friendly browser offering users robust anti-surveillance and censorship circumvention features through seamless access to the Tor network. Once a year, the Tor Project migrates the Tor Browser to the latest Extended Support Release (ESR) version of Firefox, intensive maintenance that is critical to the ongoing security, stability, and resilience of the Tor Browser.

OTF supported the 2025 Tor Browser ESR transition, which included pushing critical updates, performing an in-depth audit of Firefox ESR to assess any privacy and security impacts to the Tor Browser, managing upstream design changes, performing a quality assurance process, and releasing it to the public.

OpenVPN Maintenance and Sustainability

$199,426

Mandelbit SRL

OpenVPN — one of the most widely used VPN systems in the world — is more than 20 years old and is maintained by a small community of contributors. This project supported sustainability objectives focused on growing OpenVPN's core contributor base, improving its documentation and plans, and ensuring community ownership of core infrastructure. With support from OTF, the project was able to retain core contributors and bring on three new ones, resulting in an increase in response times to security bugs, and an improvement in the protocol's overall sustainability and security.

DEfO-Sustain

$135,520

Tolerant Networks, Ltd.

Encrypted ClientHello (ECH) plugs a privacy-hole in the Transport Layer Security (TLS) protocol by hiding previously visible details from observers. The most important, newly shielded detail is the name of the website a user wishes to visit, which (when visible) provides a straightforward method for authoritarian censors to block websites and internet services. The DEfO project develops implementations of the ECH mechanism for OpenSSL, Conscrypt, and — via those software libraries — a range of ECH-enabled web servers and clients. Support from OTF helped this project ensure ECH code remained updated, push ECH to more TLS projects, support developers implementing ECH, and perform ongoing testing and monitoring.

Information Controls Research

The Information Controls Research Program supports researchers examining how authoritarian governments are restricting the free flow of information, cutting off access to the open internet, and implementing censorship mechanisms.

Mapping DNS Trends in Latin America

$110,000

Universidad Católica del Uruguay

OTF worked with Universidad Católica del Uruguay to support five researchers investigating how internet blocking practices are being undertaken in Latin America, including the technical and strategic rationales employed by different ISPs and network operators. They also identified the main Domain Name System (DNS) blocking practices and methods currently being used by ISPs and network operators in the region. This research will help circumvention tool developers better understand the technical aspects of censorship in the Latin American context.

SHARE Youth: Digital Rights and Internet Research Program

$105,600

SHARE Foundation

The SHARE Foundation's OTF-funded Digital Rights and Internet Research program supported research on the technical capabilities of modern spyware. Researchers published four blog posts about the technical design and operational functionality of the recently discovered Android spyware NoviSpy, which has been used to surveil civil society members.

Examining the Scale of DNS-Based Censorship in India

$94,000

Karan Saini

This ongoing project is examining the scale of DNS-based web censorship in India by collecting measurements through direct and remote vantage points across various Indian ISPs. These measurements will provide greater transparency about the scale and nature of DNS censorship by producing raw datasets, block lists, and censorship signatures. The researcher is also using OTF support to develop an open source tool to automate the workflows involved in performing large-scale DNS censorship research.

Mapping Supply Chains of Information Control and Surveillance Technologies

$94,000

Yung Au

As authoritarian governments exploit the proliferation of commercial spyware and censorship tools to target civil society within and beyond their borders, mapping the supply chains of the key technologies that make these repressive tactics possible is key to intervention. This project mapped the supply chains of several repressive surveillance technologies — tracing their funding and development phases, the data pipelines they rely on, their sale and deployment, as well as the feedback loops that contribute to their continued development. It also identified various points of intervention to regulate and disrupt such supply chains, including before initial deployment and before harm is incurred.

Measuring Emerging Regional TLS Censorship in China

$94,000

Anonymous ICRP Researcher

This project investigated the emerging trend of regional TLS-based censorship in China. It developed a tool to collect and analyze data from regional middleboxes (devices that inspect network traffic) in Henan province, where a regional firewall was recently discovered, and monitored forms of censorship across three different regions in China. The published research from this project includes effective strategies to bypass this emerging system in Henan, which have already been implemented in various popular circumvention tools.

Myanmar Surveillance Research

$94,000

Anonymous ICRP Researcher

Over the last four years of military rule in Myanmar, the State Administration Council has increasingly weaponized technology to surveil, control, and intimidate the civilian population. With OTF funding, this ongoing research is examining two phases of Myanmar's technological repression: (1) surveillance technologies used for monitoring and targeting individuals, and (2) forensic technologies deployed for evidence extraction once individuals are in custody. By providing a comprehensive, evidence-based analysis of the specific interception technologies and tools enabling the State Administration Council's repressive practices, the project will shed light on effective circumvention strategies for people in Myanmar.

Digital Surveillance Inside and Outside of Myanmar

$94,000

Benedict Mette-Starke

Five years after the coup in Myanmar, repressive digital surveillance continues to expand within and beyond the country's borders. However, there has been a comparative lack of attention to how this surveillance is carried out transnationally. To fill this gap, the researcher is collaborating with Myanmar Internet Project to create a dashboard of the methods used both within the country and abroad. The dashboard will inform the development of privacy-enhancing technologies and digital security best practices for at-risk communities.

Surveillance Technologies in the Latin American Southern Cone

$94,000

Manuel Rubio

Across much of Latin America, there is a notable lack of clarity regarding the legal frameworks governing data collection on citizens, the entities involved, the equipment and technology employed, and the potential applications of this gathered information. This project identified and analyzed digital threats to civil society in the region, with a specific focus on the growing use of surveillance technology to monitor political rallies and demonstrations. The project's Surveillance Watch website sheds light on the surveillance capabilities, patterns, and targets in the region. This will help civil society better understand the threat landscape and devise effective mitigation strategies. In addition, the methodology developed in this research will be useful for research in other contexts with stringent information controls.

Investigating the Victimization of Oblivious VPN Users

$85,579

University of New Mexico

VPNs are an essential tool for accessing the free and open internet from within repressive contexts. However, if VPN endpoints are compromised, attackers can evade detection by hiding behind VPNs. Compromised endpoints can also negatively impact the user experience, which may deter further usage. For example, users might be added to industrial blacklists or subject to frequent challenges brought about by website security measures. This ongoing project is examining the impact of compromised endpoints on the user experience and evaluating the existing measures VPN service providers take to prevent malicious use of endpoints. The project is also researching best practices for addressing these challenges, with the goal of developing guidelines that can help organizations and users better protect their networks and data when using VPNs.

Exploring the Censorship Landscape of Generative AI Tools in Authoritarian Nation-States

$70,500

Anonymous ICRP Researcher

The proliferation of Large Language Models (LLMs) has brought about a shift in the online information ecosystem, as these tools present a novel information source. In authoritarian nation-states with stringent information controls, such as China, monitoring and deploying these models poses a compliance challenge to service providers, as they are beholden to a rigid set of communication and information directives. This project identified specific implementations of censorship in five LLM services hosted in China. It then developed circumvention methods to bypass them in order to support information integrity within these models and their subsequent deployments.

Broadcasting Entity Support

OTF's Broadcasting Entity Support initiatives provide innovative privacy-enhancing and censorship circumvention solutions tailored for broadcast networks and their journalists.

Media Resilience Project

$459,145

Gazzetta

The Media Resilience Project worked with independent media operating in repressive information contexts to improve digital publishing, and support secure reporting and content distribution strategies. It developed a comprehensive training syllabus for exiled journalists on using platforms and networks that provide security and resistance to censorship. A global news industry association incorporated the syllabus into their trainings, and more than a dozen newsrooms were trained directly.

Tor Secure Access Maintenance Package

$406,674

Tor Project

Tor .onion addresses have proven to be one of the most successful mechanisms for secure censorship circumvention. In this project, Tor provided the "Tor Secure Access Package" for each United States Agency for Global Media (USAGM) entity's website so audiences in censored and surveilled environments can easily continue to access USAGM network content.

Pangea-OutlineVPN Servers

$40,101

ASL19

Outline is a censorship circumvention platform that has proven to be effective in repressive information environments. In this project, technologists at ASL19, an internet freedom and exiled media organization, integrated Outline/Beepass VPN servers into Pangea, the content management system used by a number of USAGM entities, to more cost effectively circumvent authoritarian censorship.

Digital Security Animation Integration

$15,246

Small Media Foundation

This project integrated 12 animated digital security training videos (see the following project description) into a publicly available course on Advocacy Assembly, a free online training platform widely used by civil society and media organizations.

Digital Security Resource for USAGM Journalists

$2,000

Aisuluu Tekimbaeva

This project created 12 animated digital security training videos in English, Kyrgyz, Latin-American Spanish, Russian, and West-African French on common, frequently asked digital security and anti-censorship questions. This resource was designed to support USAGM network audiences to access media resources safely and securely.

OTF Resource Labs

OTF Resource Labs provide expert services to internet freedom projects. From security and usability audits to accessibility and user adoption strategy, the Labs ensure internet freedom projects are as effective, secure, and accessible as possible.

Security Lab

The Security Lab strengthens the security of open source internet freedom software by providing security audits, advancing project software security best practices, validating project privacy and security claims, and more. These services ensure the code, data, and people behind each project have the tools they need to create a safer experience for those subject to repressive information controls online. During the period covered by FY 2024 funding, the Lab performed 19 audits — improving the security of vital internet freedom technology.

Atredis Partners

$250,000

Atredis Partners, LLC

Atredis Partners performs advanced, research-driven penetration testing on a wide variety of targets (ranging from mobile to embedded, to complex applications and cloud services), and also advises clients on emerging threats and complex information risk. With OTF support, Atredis Partners provided security services for web applications, cryptography services, and adversarial audits.

Security Research Labs

$219,600

SR Security Research Labs GmbH

Security Research Labs is a security think tank with expertise in encryption, mobile and web application hacking, fuzzing, code review, and organizational security. With OTF funding, they provided security services for web applications, cryptography services, and adversarial audits.

0xche

$200,000

InfosecLabs LLC

0xche conducts security engagements, specializing in the Latin American region. The organization's focus relies on reverse engineering and penetration testing applications (web, mobile, and desktop), networks, and physical devices. 0xche also conducts vulnerability assessments, technical research, training, and source code audits for civil society organizations. 0xche provided OTF-funded projects with security services for web applications, cryptography services, and adversarial audits.

7ASecurity

$200,000

7ASecurity

7ASecurity is a team of highly skilled security professionals who conduct sophisticated audits to identify security vulnerabilities. The organization tests against all kinds of web applications, online services, hardware interfaces, mobile applications, libraries, and cryptographic tools. Their approach has informed the standard by which internet freedom tools are audited. With OTF funding, 7ASecurity provided security services for web applications, cryptography services, and adversarial audits.

Radically Open Security

$200,000

Radically Open Security

Radically Open Security is a nonprofit computer security consultancy that performs code audits, penetration tests, cryptographic audits, systems and networks audits, as well as organizational and operational security training. With OTF support, the consultancy provided internet freedom projects with professional audits of programming code, penetration testing of systems and networks, organizational and operational security training, and detailed reporting on findings alongside recommended solutions.

Assured

$190,000

Assured AB

Assured is a security consultancy that specializes in a wide range of services, including penetration testing and security assessments for web and mobile applications, information technology/operational technology/cloud infrastructure, active directory environments, Internet of Things (IoT) devices, and embedded and automotive systems.

With OTF support, they strengthened the security of internet freedom tools through adversary simulation and assessments of projects' capabilities to detect and respond to vulnerabilities.

Include Security

$100,000

Include Security

Include Security has worked with clients on more than 200 security audits, specializing in Grey Box security assessments. These assessments are conducted when the consultant has partial access to a working instance of an application and its source code, improving consultants' efficiency in finding vulnerabilities. Include Security provided OTF-funded projects with security services for web applications, cryptography services, and adversarial audits.

NimKat

$100,000

NimKat

NimKat provides expert guidance on digital security best practices, institutional policies, open source IT infrastructure, and risk analysis and mitigation through organizational digital security audits. As part of OTF's Security Lab, the organization provided security services for web applications, cryptography services, and adversarial audits.

User Experience & Discovery Lab

The User Experience & Discovery (UXD) Lab provides user experience research and design support to technology-focused internet freedom projects. This includes secure usability and user-interface assistance, as well as accessibility assessments for internet freedom and digital security tools. The services help to strengthen projects' understanding of the needs of their user communities, inform the usable and context-appropriate design of the technologies they are building, and solve accessibility challenges that could hamper tool adoption in repressive information contexts. During the period covered, the Lab supported 45 usability and accessibility support engagements.

Superbloom Design

$182,000

Superbloom Design

Superbloom is a nonprofit organization focused on user experience design. With OTF support, the vendor provided usability design and user research support to internet freedom tools.

Plaintext Design

$155,077

interalia gGmbH

Plaintext Design supports development teams with user research and user experience design to improve the usability and accessibility of internet freedom tools. With OTF funding, Plaintext Design provided design support to a number of internet freedom privacy and security tools.

Ura Design

$150,000

Ura Design

Ura Design provides user experience (UX), accessibility, visual communication, and innovative design services. With OTF support, the vendor provided crucial UX support and usability testing for internet freedom tools.

Okthanks

$149,982

OkThanks LLC

Okthanks offers user research and user experience design support to internet freedom tools, improving their usability and accessibility. With OTF support, Okthanks provided UX and discovery research support to shutdown-resistant tools and other internet freedom technologies.

The Engine Room

$125,000

The Engine Room

The Engine Room delivers user research and UX design support in order to improve the usability and accessibility of internet freedom tools. With OTF support, the vendor delivered comprehensive UX research for threat intelligence tools and other internet freedom technologies.

Localization Lab

$125,000

Localization Lab

Localization Lab helps localize and adapt internet freedom tools to meet user needs, improving the tools' usability and accessibility. With OTF support, the vendor carried out user-centered research for several internet freedom technologies.

Convocation Research & Design

$104,000

Superbloom Design

Convocation Research and Design is a security and research design agency that helps improve the usability and accessibility of internet freedom tools. With OTF support, the vendor helped internet freedom projects better understand user needs.

---

tin.fyi

$100,000

tin.fyi

tin.fyi offers user research and UX design support in order to improve the usability and accessibility of internet freedom tools. With OTF support, the vendor helped internet freedom tools assess and improve the user experience.

Technique

$100,000

Technique UX LLC

Technique delivers user research and UX design support, improving the usability and accessibility of internet freedom tools. With OTF support, the vendor provided privacy-focused user research to internet freedom projects.

Accessibility Lab

$94,226

A11y Lab

Accessibility Lab is a digital accessibility organization with expertise in comprehensive accessibility audits, inclusive design and development, and specialized training. With OTF support, Accessibility Lab conducted website accessibility audits and training for internet freedom projects to increase utility and adoption in repressive information environments.

Impact & Engagement Lab

The Impact & Engagement Lab helps technology-focused internet freedom projects effectively communicate about their work in order to contribute to audience adoption in the world's most information repressive contexts. It also shares the knowledge created through projects so others can iterate and build on their work to advance internet freedom.

Kumquat

$100,000

Kumquat

Kumquat specializes in branding and graphic design for purpose-driven organizations. As an Impact & Engagement Lab vendor, they helped internet freedom technology projects leverage data visualization and design to effectively communicate the impact of their work, leading to greater adoption.

Ura Design

$100,000

Ura Design

Ura Design is a design collective focused on open source, secure, and privacy-preserving internet freedom projects. As a Lab vendor, they helped internet freedom technology projects leverage data visualization and graphic design to effectively communicate about their work, leading to greater adoption.

Curious Shapes

$80,000

Curious Shapes

Curious Shapes is a communications consultancy whose staff have an extensive global network and significant expertise operating in information repressive contexts on internet freedom issues and programs. The vendor provided editorial services to internet freedom technology projects to help them effectively communicate the impact of their work, leading to greater adoption.

Global Voices

$80,000

Global Voices

Global Voices is an international, multilingual community of writers, translators, and human rights advocates. The vendor provided editorial services to internet freedom technology projects to help them effectively communicate the impact of their work, leading to greater adoption.

Christy and The Moon Tide Collective

$50,000

Christy and The Moon Tide Collective

Christy and The Moon Tide Collective comprises writers, researchers, and strategists that support civil society. The vendor provided editorial services to internet freedom technology projects to help them effectively communicate the impact of their work, leading to greater adoption.

Tynymgul Eshieva

$50,000

Tynymgul Eshieva

Tynymgul Eshieva specializes in creating impactful visual content that educates and empowers diverse audiences. The vendor helped internet freedom technology projects leverage design to effectively communicate the impact of their work, leading to greater adoption.

Vaibhav Bhawsar

$25,546

Vaibhav Bhawsar

Vaibhav Bhawsar is a designer and technologist. His work helped internet freedom technologies leverage design and data visualization to effectively communicate the impact of their project, leading to greater adoption.

OPEN TECHNOLOGY FUND

FY 2024

ANNUAL REPORT