The Information Safety & Capacity (ISC) Project

FINAL REPORT
2011-2020

Submitted to: USAID/DCHA

Submitted by: Counterpart International

Table of Contents

Acronyms List

2FA	two-factor authentication
APS	Annual Program Statement
CSO	civil society organization
DDoS	Distributed Denial-of-Service Attack
DRL	US Department of State's Bureau of Democracy, Human Rights, and Labor
DSS	Digital Security Specialist
FY	Fiscal Year
GCSS	Global Civil Society Strengthening
ICT	information & communications technology
IFPA	Internet Freedom & Policy Advocacy
IGIF	Internet Governance Internet Freedom
ISC	Information Safety & Capacity Project
ISP	Internet service provider
KMP	Knowledge Management Portal
LGBTQ	Lesbian, Gay, Bisexual, Transgender, Queer
MEL	Monitoring, Evaluation, & Learning
NED	National Endowment for Democracy
NGO	non-governmental organization
NSO	NSO Group Technologies, an Israeli technology firm whose spyware (Pegasus) enables the remote surveillance of smartphones
OS	Operating System
OSF	Open Society Foundations
OTF	Open Technology Fund
PDP	privacy and data protection
PGP	Pretty Good Privacy, encryption for e-mail
POTS/PSTN	Plain Old Telephone Service / Public Switched Telephone Network
PQL	Program Quality & Learning
RFA	Request for Applications
TLS	Transport Layer Security
Tor	The Onion Router, multi-hop proxy-server anonymous web browsing
ToT	Training of Trainers
UPR	Universal Periodic Review
USB	Universal Serial Bus
VPN	virtual private network

Executive Summary

Introduction

Over the past decade, civil society organizations (CSOs) have been increasingly targeted by the same malicious cyber campaigns as private citizens, corporations, and governments, threatening not only freedom of expression but democracy itself. Though transformations in technology have no doubt revolutionized the global communications ecosystem in myriad positive ways, state-backed digital espionage has been increasingly used to silence or discredit journalists, activists, and humanitarian groups around the world. More importantly, while CSOs face the same sophisticated threats as large companies, they rarely have the resources required to build up resilience or enlist outside help, leaving them increasingly vulnerable as these threats continue to evolve.

As early as 2008, the US Department of State's Bureau of Democracy, Human Rights, and Labor (DRL) financed Internews and Freedom House to implement cybersecurity as aid trainings in support of internet freedom. Having determined those resources to have been well-spent, the US Congress subsequently expanded its internet freedom earmark to allocate resources to the US Agency for Global Media (formerly the Board of Broadcasting Governors), which – in collaboration with Radio Free Asia – created the Open Technology Fund (OTF) to finance the development of technology to support activists, as well as to USAID, which in turn granted USD 24 million over multiple years to fund the **Information Safety & Capacity Project** (ISC).

Designed and implemented by **Counterpart International** to protect the online safety of developing-world civil society, including non-governmental organizations and independent media outlets, the ISC was launched in October 2011 with a distinct mission to strengthen the cybersecurity defenses of thousands of activists and journalists in dozens of countries. In later years, the addition of pro-cyberliberty policy advocacy to the ISC's mandate further broadened its support for civil society, including strengthening the work of policy advocates and the advocacy capacity of non-governmental organizations (NGOs), and improving regulatory environments that determine online freedom.

After achieving its primary mission to strengthen the cybersecurity defenses of thousands of activists and journalists in dozens of countries, ISC was also able to successfully finance technology upgrades across a broad range of Local Partners, build awareness and community through the convening of annual workshops, and support grass roots advocacy for cyber liberty.

Achievements and Milestones

9,852 local civil society activists and journalists trained by Digital Security Specialists to respond to acute cyber threats, including surveillance, data loss, phishing, malware, insecure websites, and outdated software.

14 policy papers, 3 new cybersecurity laws, and 8 judicial monitoring reports were – respectively – published, drafted, and developed by ISC's Internet Freedom Policy Advocacy partners, who also led more than **60 roundtable discussions** and consultations with relevant policymakers.

1,487 Local Partners across 36 countries, having received support from ISC, now utilize encrypted messaging, secure browsers and networks, and licensed software.

47 country assessment reports produced by ISC to evaluate information security threats, cyber-surveillance, cyber-attacks, and censorship continue to help inform programming undertaken by USAID Missions and other Local Partners.

348 local cybersecurity experts benefitted from ISC's Training of Trainers (ToT) program, enabling the continuation of critical capacity-building among Local Partners.

Indigenous language resources, as well as gender-based guidelines for women journalists facing cyberbullying and censorship, were created by ISC's digital security specialists, who also provided specialized support to address heightened security risks to these groups within society.

26 bespoke digital security tools tested, translated and / or customized to better protect journalists and activists throughout the developing world.

USD $216,823 in-kind grants provided to fund critical hardware and software updates.

4 proprietary technology tools developed to address digital security issues frequently faced by ISC's Local Partners.

9,582

local civil society activists and journalists trained by Digital Security Specialists to respond to acute cyber threats, including surveillance, data loss, phishing, malware, insecure websites, and outdated software.

1,487

local partners throughout **36 countries** now utilize encrypted messaging

348

local cybersecurity experts produced through the **Training of Trainers program**

14

policy papers published

47

country assessment reports produced

26

digital security tools supported via testing, translation, and customization

Investing in Trust

Successful cybersecurity depends not only on adopting defensive solutions, but also on the end user's trust in the person providing assistance. Initially, responsibility for selecting countries in which to work required obtaining permission from the relevant USAID mission, which ultimately tracked back to USAID's Bureau for Democracy, Conflict and Humanitarian Assistance (DCHA) itself, reducing ISC's influence in the process. Over time, however, Counterpart became more proactive in proposing new ISC countries, enabling the ISC Chief of Party to adapt to working with the ISC Agreement Officer Representative to identify new countries, initiate mission clearance requests, and shepherd requests through the approval process.

From there, the ISC identified Digital Security Specialists who were chosen in part based on the strength of their relationships with in-country activists, NGOs, journalists and the wider media. The differences among these specialists were an asset to the project, and meant no single cybersecurity auditing mechanism was forced upon staff. In general, each ISC cybersecurity assessment began with learning from the Local Partner what they cared about defending.

Ultimately, good communication and the establishment of trust – first with the Mission and later with Digital Security Specialists and Local Partners – proved a critical component of Counterpart's success.

Initial Threats and Fixes

At the start of the ISC in 2011, threats resulting from compromised online communications, such as endpoint protection that safeguards PCs from malware and account security that prevents attackers from logging into Gmail and Facebook accounts, made up the majority of digital security issues. As many of these proved unable to be easily mitigated by off-the-shelf hardware, software, or services, much of the ISC's initial work focused on teaching beneficiaries how to use specialized third-party solutions to secure their data. Over time, however, as threats became more complex, the effectiveness of these solutions diminished and people reverted to old, non-secure behaviors.

With the increased threats, however, came an increase in awareness about the importance of safeguarding civil society. Other stakeholders, including technology companies and institutional donors, stepped in to help build, integrate, and automate solutions that facilitated defensive measures. In the end, however, much of the progress made to address the early threats in cybersecurity were as much due to the migration from PCs to smartphones to transmit data, as the collective efforts of the ISC and others. Simply put, today's smartphone operating systems (iOS, Android) are much more secure than PC operating systems (Windows, macOS), offering whole-hard-drive encryption as a default setting, as well as access via biometric authentication that auto-updates, such as fingerprint and facial recognition authentication.

State Actors and Suppression

Though instrumental in building both awareness and capacity among thousands of Local Partners and specialists, the ISC ultimately faced a more complex challenge. In the early 2010s, repressive regimes and their law enforcement agencies were not nearly as adept at using digital espionage to suppress dissent and stifle opposition at home and abroad.

By 2015, this was no longer the case. The increasing presence of the internet in everyday life meant the presence or absence of cyber policy affected nearly everything. Cyber policy advocacy had matured as people became increasingly aware of online threats and were willing to voice concerns about digital platforms being used for increased government surveillance. Internet policy also evolved as countries increasingly adopted frameworks for national cybersecurity that – intentionally or not – often legitimized the deployment of resources to law enforcement, which in turn posed additional threats to civil society who were then faced with a greater need to be vigilant regarding cybersurveillance.

Though the ISC's original design did not include engagement in policy advocacy, midway through, USAID requested that policy work be added to its mandate. After its relatively tentative start in earlier years, supporting research and society-facing activities under the banner of Internet Governance Internet Freedom (IGIF), the ISC successfully pivoted to government-facing policy advocacy.

Initial projects eased the ISC into cyber policy, including subawards to support research that could be used by advocates to demonstrate to policymakers the importance of increased online freedom. Resources were also allocated to finance public information campaigns to inform citizens of the importance of defending and promoting digital rights. During the ISC's final year of implementation, the ISC recalibrated by renaming this work Internet Freedom Policy Advocacy (IFPA), issuing a global Annual Program Statement (APS) calling for proposals to support government-facing advocacy. Of the 50 applications the IFPA APS received, ISC made subawards to ten local NGOs in as many countries. Counterpart augmented IFPA's financial support with mentoring for subawardees.

While all IFPA work focused on domestic cyber policy in developing countries, subawardees focused their work in different ways, including advocating for the adoption or amendment of a specific law, regulatory change or enforcement, the training of judges, strategic litigation, or privacy, surveillance, and cybercrime. Overall, the organizations supported by IFPA–many of whom which have already made great gains that bode well for the road ahead–have continued to work on policy change goals, undeterred by the long timeline often needed to affect legislation.

IFPA subawardees produced 14 policy papers, 3 draft laws, and 8 position or monitoring papers, in addition to hosting 59 roundtables, online discussions, and one-on-one meetings with parliamentarians, judiciaries, and other stakeholders to advance cyberliberty agendas. In 2020, the Thomson Reuters Foundation honored ISC IFPA subawardee Fundamedios (Ecuador) with the TrustLaw Collaboration Award 2020 for its work drafting two new pieces of legislation, the Personal Data Protection Act and Access to Public Information Act.

In the end, IFPA-like support for policy advocacy raised the visibility of key issues, advanced pro-freedom policy, and increased local civil society advocacy capacity, all while drawing new players into the pro-good-government field who, per Counterpart's past experience, will likely end up becoming MPs, regulators, or presidential advisors.

Looking Ahead

Targeted digital threats to CSOs are not a local problem limited to authoritarian countries, but a global threat as these regimes increasingly target civil society across borders. Simply put, cybercrime has exploded to the point of becoming a national security concern, which in turn has catalyzed an escalating arms race in cyberspace as governments scale up capabilities to fight and win wars in this domain. Telecommunication companies, Internet service providers (ISPs), and other private sector actors now actively police the internet, and calls for the regulation of global networks of information and communications have never been greater. States – once thought to be powerless in the face of the internet – have taken these tools into their own hands.

At the same time, technological development has created new opportunities for surveillance and espionage that circumvent existing regulatory frameworks, such as private sector development of commercial spyware. This also puts civil society in peril, as evidenced by the controversies around spyware providers like NSO Group Technologies (NSO) selling capabilities on par with leading intelligence agencies to several authoritarian regimes. Worse still, as compromises affecting CSOs rarely result in financial damage, they are both difficult to quantify, and often result in the erosion of trust within a community as citizen's accounts are compromised and used to spread malware over social networks.

While the evolution of the ISC and the support of other stakeholders is critically important going forward, how governments react to these threats and challenges will ultimately determine the future of cyberspace, and by extension the communications platforms upon which global civic networks depend. Since civil society is vital to a functioning democracy, the trend of authoritarian regimes projecting power abroad through digital means is an assault on democracy itself. Continuing to broaden the field of support, as well as maintaining and expanding existing networks affected by the ISC is key.

Part 1: ISC Project Vision and Strategy

The Importance of Cybersecurity in Civil Society

The more authoritarian the government, the more resources its law enforcement agencies are likely to dedicate to inhibiting civil society. Thirty years ago, that meant curbing activists on the ground in real-time. With the advent of information and communications technology (ICT) – progressing from personal computers to the internet, mobile telephony and, most recently, smartphones – the stakes have both increased and broadened, particularly for civil society actors in developing countries.

Being relatively small and nimble – particularly when compared with law enforcement agencies – civil society organizations have proved not only effective at carrying forward pro-rights struggles online, but have used the internet to campaign and deliver news in ways that bypass government controls of traditional media, including printing presses, newspaper distribution networks, television and radio transmitters, and frequencies.

Initially, developing-world governments, many of which had long professed a commitment to liberty while simultaneously detaining, persecuting, prosecuting, and imprisoning activists and journalists, were at a loss as to how to harness and implement advances in ICT. However, beginning in the 2000s and accelerating over the subsequent decade, governments realized that by controlling communication lines going in and out of a country they could use technology (initially Western, and later Chinese and Russian) to monitor unencrypted internet traffic for the purposes of surveilling citizens and ultimately identifying and even eliminating those who challenged their authority. As a result, governments aggressively sought to procure offensive hacking tools developed by companies such as HackingTeam, Gamma, and NSO, while at the same time developing the capacity – either in-house or with the help of independent contractors – to hack those they considered threats to their hold on power.

To avoid being compromised, civil society actors (inclusive of civil society organizations (CSOs), NGOs, and independent media)–particularly in more authoritarian countries—were compelled to continually up their cybersecurity defense game. First-world technologists responded by creating a bevy of tools, such as Pretty Good Privacy (PGP), an encryption platform for e-mail, Off The Record, an encryption platform for instant messaging, The Onion Router (Tor), open-source software for enabling anonymous communication over the internet, and TrueCrypt, an encryption platform for data stored that helps protect potentially vulnerable data and communications.

International human-rights organizations, including the UK's Tactical Technologies Collective and Ireland's Frontline Defenders developed online guides to support activist awareness of both threats and solutions, while grant-making organizations – early donors in this space, such as Open Society Foundations (OSF), the National Endowment for Democracy (NED), the Dutch Foreign Ministry, and the Swedish International Development Cooperation Agency– financed civil society cybersecurity workshops. In 2008, DRL financed Internews and Freedom House to implement cybersecurity as aid trainings in support of internet freedom. Having determined those resources to have been well-spent, the US Congress subsequently expanded its internet freedom earmark to allocate resources to the US Agency for Global Media, which – in collaboration with Radio Free Asia – created the OTF to finance the development of technology to support activists, as well as USAID, which in turn launched the ISC to scale cybersecurity for civil society work in dozens of countries around the world

Naturally, the more successful online activism became, the greater the lengths authoritarian governments went to impede it. Though Western tech companies constantly develop and upgrade online tools to better enable activists in their work—via Facebook, Twitter, Gmail, Apple's iTunes and Google Play—authoritarian governments have successfully pressured service-providers to participate in cracking down on social activism, be it by subpoenaing information about user identities, censoring undesirable content, or blocking access to objectionable applications and virtual private networks (VPNs).

As a result, provisioning cybersecurity assistance to developing-world civil society has become a key pillar of support for activists and journalists working in dangerous places to organize citizen opposition to injustices of all kinds, and expose exploitive government policies that benefit elites rather than promote socio-economic equality. By training activists and journalists to protect their data and communications, projects like the ISC have helped to facilitate global netizens to educate citizens about their rights (or lack thereof), hold governments to account, and defend those whose voices have been silenced – from marginalized communities to environmental champions.

Global Threats and Trends: Old and New

A core tenet of USAID's good governance portfolio involves strengthening and supporting civil society, inclusive of independent media, in developing countries. As authoritarian governments increased their use of technology to surveil citizens and organizations perceived to threaten their hold on power, activists and journalists have come to rely on ever-improving defensive cybersecurity to ensure their ability to safely advocate for freedom and provide news and information to a broader citizenry. Though the initial training of civil society actors was helpful, the work of CSOs and independent media continued to be significantly impeded by inadequate cybersecurity literacy and capacity.

To more proactively support civil society's capacity to defend itself against hostile surveillance that frequently placed activists and journalists in harm's way, suggestions were solicited from members of Global Civil Society Strengthening (GCSS), the USAID-funded program under a Leader with Associates Cooperative Agreement. The result was the development of the ISC.

In its nine years, during which time cybersecurity threats have evolved significantly, the ISC has successfully developed and implemented myriad cybersecurity defense activities, as well as increasingly innovative solutions to mitigate threats and raise awareness about new and emerging technologies.

Cybersecurity Threats in the Beginning

At the start of the ISC in 2011, threats resulting from compromised online communications, such as endpoint protection that safeguards PCs from malware and account security that prevents attackers from logging into Gmail and Facebook accounts, made up the majority of digital security issues. As many of these proved unable to be easily mitigated by off-the-shelf hardware, software, or services, much of the ISC's initial work focused on teaching beneficiaries how to use specialized third-party solutions to secure their data. Over time, however, as threats became more complex, the effectiveness of these solutions diminished and people reverted to old, non-secure behavior.

In response, the ISC continually worked to ensure Local Partners' staff were well-versed in cybersecurity defense. Digital Security Specialists tend to have a relatively short and focused checklist of minimum necessary fixes for cybersecurity vulnerabilities, including converting pirated software to licensed software, ensuring comprehensive hard-disk encryption in operating systems, and enabling two-factor authentication (2FA) in online account settings and control panels. Because these fixes leverage features that are now built into tools and services used by many of ISC's beneficiaries—including activists and journalists who use them as a matter of routine—the ISC is now able to "set and forget" fixes for its Local Partners without relying on an end user learning new protocols, changing their practices, or facing decisions that could be misinterpreted.

Evolution of Threats Through Technological Innovation

As cybersecurity threats became more mainstream, both technology companies and institutional donors stepped in to help build, integrate, and automate solutions that facilitate defensive solutions, though more recent innovations in technology have, to a large extent, fixed the problems. Most new smartphones automatically encrypt locally stored data, most users have transitioned from unencrypted SMS to encrypted messaging applications such as WhatsApp and Signal, and most websites have upgraded from unencrypted HTTP to encrypted HTTPS.

In fact, much of the progress in cybersecurity during the ISC's life had as much to do with the migration from PCs to smartphones to transmit data, as many of the behaviors that were previously complex or difficult for users to adopt are now automatically enabled. Today's smartphone operating systems (iOS, Android) are much more secure than PC operating systems (Windows, macOS), offering whole-hard-drive encryption as a default setting, as well as access via biometric authentication – such as fingerprint and face ID. They are also mainly open-source, with applications auto-updating – meaning piracy on smartphones is no longer the problem it once was.

Another major IT evolution that positively impacted cybersecurity is the ever-increasing availability of cloud services. While these are not impervious to attack, a well-defended online account – such as data storage – has the advantage of storing so much data that it is not obvious to an attacker where to start. In cases where the target is known to the attacker, hacking through Google or Facebook's online security is significantly more difficult than trying to access data carelessly stored on an external drive.

Despite the continued attempts by adversaries to exploit simple vulnerabilities with tactics such as password spraying (an effective attack given people often re-use credential pairs across platforms), surveillance of online traffic using monitoring systems installed at ISPs, and delivery of ransomware in booby-trapped phishing emails, the ISC was able to successfully immunize its beneficiaries against cyberattacks from governments and cybercriminals by empowering them with relatively simple defenses (described in detail in the ISC's *Cybersecurity Threat Model*) and following up to ensure these were consistently kept enabled. An adversary is likely to find launching a cyberattack on an ISC beneficiary is too expensive, and will instead attack an undefended target, or resort to other tools of intimidation.

In the early 2010s, law enforcement agencies posed different dangers than they do today. As such, for the first few years the ISC's model emphasized evaluating cybersecurity threats on a country-by-country basis and calibrating solutions to defend activists and journalists based on their specific environment. By the end of the ISC's implementation period, cybersecurity threats that were once unique to certain countries became more universal, resulting in developing-world CSOs and media organizations facing a more diverse range of attacks – far more so than a decade ago. For defense strategists like the ISC, cybersecurity has become more complicated and the scope of threats broader. To effectively combat this ever-changing landscape, the ISC adapted to apply a relatively uniform set of defensive tools and techniques in every country where it works in order to establish a baseline of cybersecurity for its Local Partners.

The ISC Project's Network of Digital Security Specialists

The ISC focused on three cybersecurity defense vectors: (1) **eliminate the insecurities** of activists and journalists; (2) **educate people** to ensure they have the knowledge and tools to defend themselves against cybersecurity threats; and (3) **create local teams and a network of experts** to continue to provide cybersecurity support.

To achieve these, the ISC developed Digital Security Specialists who led work on the first and second vectors and, over the life of the project:

- provided support to 1,487 local partner organizations across 36 countries
- trained 9,852 local civil society activists and journalists – 62% of whom were women – to respond to cyberthreats
- hosted 41 regional workshops

To address the third vector, which was foundational to the ISC's sustainability, Digital Security Specialists and Regional Managers identified local cybersecurity experts to support ISC's Local Partners, as well as newly emerging civic space actors, to employ and maintain cybersecurity protocols. ISC built the capacity of 348 local cybersecurity experts through the Training of Trainers (ToT) program.

Cybersecurity Defense Vectors:

1. Eliminate Insecurities
2. Educate People
3. Create Local Teams and a Network of Experts

ISC Digital Security Specialist Achievements

SUPPORTED

1,487 local partner organizations

36 countries

TRAINED

9,852 local civil society activists

62% were women

HOSTED

41 regional workshops

The ISC Project's Cybersecurity Threat Model

Defense starts with defining which assets an individual is worried about losing. In the case of civil society actors, the ISC found the primary concerns to be:

- secure communication with colleagues, journalists, donors, and friends
- operational privacy, particularly activity records, proposals, and financial information
- protection of identities of colleagues, co-organizers, sources, and supporters
- access to websites and online accounts

The ISC was staffed by cybersecurity experts and specialists who not only ran the cybersecurity workshops, but were often friends with, and thus trusted by, activists and journalists, worked with groups such as Frontline Defenders and Access Now, and stayed informed about new threats and compromises within communities. While this sort of information is not generally written down or widely shared – people and organizations who have been compromised are rarely willing to publicly acknowledge it – the ISC was able to develop a cybersecurity threat model based on experience of common compromises that resulted from five distinct types of cyberinsecurity.

Since ISC's resources were limited, efforts to provide cybersecurity within civil society focused on the simplest possible measures to address these five insecurities, including:

1. Insecurity of Online Accounts 44% of compromises

Defend all online accounts with strong passwords and employ the use of an effective and secure password manager to generate, store, auto-enter, and verify the legitimacy of login pages soliciting passwords.

Defend important accounts with 2FA e.g., a smartphone-based one-time-password generator such as Google Authenticator.

2. Insecurity of Endpoints 42% of compromises

Use only updated or patched software. Since pirate software does not get patched, it is critical to convert all platforms to licensed software in order to eliminate this insecurity (e.g., Microsoft Windows, Microsoft Office).

3. Insecurity of Data at Rest 10% of compromises

Ensure all devices – including PCs, smartphones, tablets, and thumb drives – require authentication such as PINs, swipes, passwords, fingerprints, or facial recognition.

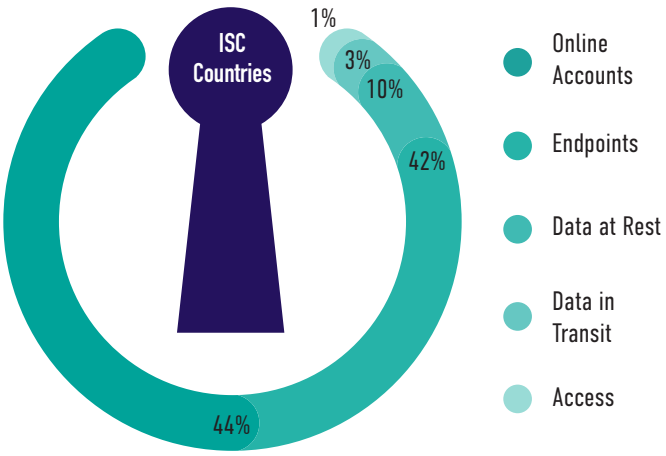
Enable whole-drive encryption for all data storage devices, including PC hard drives and SSDs, smartphone RAM, and thumb drives.

4. Insecurity of Data in Transit 3% of compromises

Stop using normal telephony, unencrypted SMS, and WeChat, which is controlled by the Chinese Government, and use encrypted applications such as Facebook Messenger, Skype, and Signal et al for all messaging, voice, and video communication.

5. Insecurity of Access 1% of compromises

Step up anti-DDOS protection on websites (e.g., Deflect, Galileo, et al), and use a VPN or proxy client to access otherwise blocked content.



By combatting compromises associated with the aforementioned insecurities, ISC's cybersecurity model was able to focus on changing the behavior of individuals and organizations to keep them and their work safe online. The ISC worked to prioritize 10 independent media organizations and 20 rights-defending NGOs that the ISC and USAID most wanted to help – e.g., ISC's Local Partners. ISC's Digital Security Specialists spent time establishing trust with these organizations and their staff, auditing their tech use to establish the most pressing vulnerabilities, and helping them mitigate each of the five insecurity types, while simultaneously communicating what, why and how ISC was helping.

By working with civil society actors closely and over a sustained period of time, the ISC expanded the number of people in each country who are informed about and able to help combat threats to cybersecurity among their colleagues and networks. Initially, 30 Local Partners proved adequate to mobilize the ISC. Over time, the Digital Security Specialists acquired a better understanding of the environment, and undertook to expand their network of Local Partners to between 45 and 100 as the initial group either was fixed or grew unresponsive, resistant, or disinterested.

The Importance of Internet Freedom Policies

Netizens' ability to work safely online and accomplish their objectives begins with technological capability and skills, but also depends on government policy – including all the things that people are or are not allowed to do, what ISPs may or may not do, the kind of competition that is encouraged or discouraged, and whether a user's fear of online threats are assuaged or stoked. The collective rubric of internet freedom policy can include government rules and their implementation related to cybercensorship, cybercrime, encryption, telecom policy, e-government, digital rights, and technical issues such as domain-name management, among other things.

For example, online service vendors may offer to pay an ISP to prioritize its traffic or de-prioritize a competitors' traffic. This may be good for an ISP's bottom line, but can be bad for consumers whose choice of online services becomes artificially skewed as a result. Similarly, online service providers are tempted to track everything users do, but this sort of excessive tracking often results in an increase in highly-targeted marketing – including political advertising – that may influence a user's preferences and perspective. Law enforcement agencies will, by definition, always want more visibility into what citizens do, see, and say. Good governance requires strong checks that encourage the establishment of probable cause, and prevent fishing expeditions and abuse, especially where the governing party's desire to retain power threatens to subvert democracy.

Policy Advocacy Responses

Policy advocacy can be divided into government-facing and society-facing, with the former operationalized by working to affect the adoption of laws (legislative), their implementation (executive), and their enforcement (judiciary). The latter, which eventually and often indirectly affects government, may include public education campaigns (media), policy workshops for key actors (students, academics, and journalists), research about which policies have what effects, and more. Thus, a policy advocate's toolbox may also include liaising directly with policymakers to help them understand the issues and the options, such as coalition-building with business or civil society actors, or strategic litigation.

Through analysis, experience, and trial and error, ISC determined the defenses for these most prominent types of cyber insecurity are effective and share the following characteristics:

- stock
- small
- cheap
- implementable
- easy for Digital Security Specialists to explain
- essential / non-negotiable
- easy to assess
- non-disruptive to the end user
- "good enough" in terms of defensive ability

Evolution of Cyber Policy

If, in 1995, cyber policy was considered somewhat nascent, by 2015 the increasing presence of the internet in everyday life meant the presence or absence of cyber policy affected nearly everything. At the same time, cyber policy advocacy matured as people became increasingly aware of online threats and were willing to voice concerns about digital platforms being used for increased government surveillance.

Internet policy also evolved as countries increasingly adopted frameworks for national cybersecurity that in turn opened gateways for legitimizing the deployment of resources to law enforcement, which posed additional threats to civil society who were faced with a need to be vigilant regarding requests for records and cybersurveillance and advocate for judicial oversight.

ISC Project's Internet Freedom Advocacy Model

Though the ISC's original design did not include engagement in policy advocacy, midway through its 9-year run, USAID requested that policy work be added to its mandate. The ISC's early years of policy engagement was relatively tentative, supporting research and society-facing activities under the banner of IGIF. As the ISC evolved, the ISC pivoted to direct government-facing policy advocacy, providing grants and technical support to Local Implementers in ten countries under the rubric IFPA.

Overall, ISC's engagement in cyberpolicy is relatively recent when compared with its cybersecurity work. A major policy trend observed during ISC implementation was the rise of privacy and data protection (PDP) as a significant issue. Since PDP is generally a netizen-defense issue, legislating it may be viewed as a positive if policy advocates are highly skilled and ready with regulatory recommendations to constrain data collection, retention, and use, while being generic enough to apply to governmental agencies and not just targeted at tech companies.

Safety for Civil Society Activity in Restricted Spaces

Development assistance often prioritizes good governance, which in turn encourages government accountability to its citizens. An important element in the equation, however, is civil society actors being free to organize and advocate for increased government transparency and accountability. The less free a country, the more important it is that civil society be able to advocate for increased freedom; conversely, the less free a country, the more difficult a government will try to make it for civil society activity to occur.

The ISC was designed to provide civil society—rights-defending activists and independent media—with enough cybersecurity assistance to be able to get on with their work without worrying about being compromised online, with the added benefit that enhanced cybersecurity also improves a citizenry's general knowledge about technology while increasing their comfort level using new tools to ensure the safety and integrity of their work.

The addition of pro-cyberliberty policy advocacy to the ISC's mandate opened new doors for supporting civil society, including strengthening the work of policy advocates and advocacy capacity of NGOs, as well as improving regulatory environments that determine online freedom. Policy work, such as that undertaken by ISC's ten IFPA subawardees, demonstrated that when advocates positively move the needle of a country's cyberfreedom environment, small changes can have dramatic impact. Sometimes policy advocates can succeed in putting in place liberty-preserving legislation about a new tech-related topic before vested interests become too powerful to oppose. Sometimes civil society will need to push back against a government's tendency to overregulate, contributing to increasingly restrictive civic space. And, sometimes campaigners can cloak a pro-freedom policy in the guise of economic development, which most governments seek to support more willingly than citizens' rights.

On average, successful policy advocacy work can take several years to implement, so the work undertaken by ISC's IFPA subawardees will be ongoing (and supported by other donors). One already visible IFPA output, however, is the introduction into Armenian parliament of PDP legislation constraining the use of personal data by telecom companies to technical necessity while mandating net neutrality at the same time.

Part Two: Evolution of the ISC Project

In 2008, the first congressionally allocated "internet freedom" funding reached the Department of State and was deployed to support the mitigation of developing-world cyber censorship, and the promotion of cybersecurity for activists and journalists, and cyber policy advocacy. When this earmark was extended to USAID and the US Agency for Global Media, USAID's allocation was put into the GCSS, led Counterpart. USAID ultimately chose to fund Counterpart's approach of augmenting cybersecurity training by proactively hiring local talent to help activists and journalists address their vulnerabilities and become cybersecure. In 2011, the ISC was launched with two additional activity areas added at USAID's request, including a small grants program to finance technologies that support internet freedom, as well as a conference to convene Western activists involved in the design, build-out, and implementation of cybersecurity-supporting tech. In 2016, halfway through ISC Project's 9-year run, USAID asked Counterpart to add cyber policy as a fourth activity.

Meeting Demand and Expanding Reach

The principles behind ISC's cybersecurity work did not change significantly over the life of the project. The priority was, and remained, identifying and neutralizing the major digital threats faced by media organizations, journalists, activists, and NGOs. The ISC's original design called for regional staff who could provide cybersecurity support in various local languages – including Russian, Spanish, and Arabic. Over time, however, the need for cybersecurity-defense services increased and the ISC evolved to its final model of engaging full-time in-country Digital Security Specialists to provide support to beneficiaries and maximize its overall reach. **By the project's end, ISC had supported 9,852 people across 1,487 organizations in 36 countries.**

Financing Technology Solutions

As the OTF project ramped up, financing for technologies became its raison d'être, and the need for the ISC to fill that niche was reduced. Consequently, the ISC's technology-financing activity was reduced to solving specific problems that ISC's staff identified as critical. Over the years, ISC technology grants were used to translate cybersecurity training courses into myriad languages, support incremental improvements of cybercircumvention tools needed to respond to new steps in censorship, improve documentation of anonymity-guaranteeing software, and develop new tools to detect compromises to devices' trusted root certificate stores.

Building Community

For its first several years, the ISC's Annual Global Workshop was a key event for internet freedom activists and technologists. Over time, however, other conferences focused on internet freedom were initiated. In addition to the Internet Governance Forum, other events were launched to support community building, such as the Internet Freedom Festival and Access Now's RightsCon. Eventually, the Annual Global Workshop offered less value to the community and in its final year was discontinued in favor of more high-value interventions such as local cybersecurity support provided by ISC's Digital Security Specialists.

Increasing Attention on the Internet

The gradually increasing role and importance played by online and digital services has been reflected in the support afforded internet related activities by the US Government, as well as USAID's expansion of its internet freedom programming and the addition of a new objective for the ISC.

The ISC's policy engagement grew incrementally, beginning with support for research into what kind of regulation netizens would welcome and the behavior of state actors across online platforms, into support for society-facing policy advocacy such as awareness raising campaigns, workshops, and cybersecurity conferences. Accordingly, ISC's leadership shifted its strategy in its final year to provide funding and technical support for NGOs engaged in government-facing advocacy for the enactment of cyberliberty policies.

Cybersecurity Support Model

The purpose of ISC's cybersecurity-defending engagement in each country was to neutralize major cybersecurity threats faced by Local Partners in-country while simultaneously embedding cybersecurity support functionality into the local environment. Having experimented with various means of accomplishing the latter across six countries in the first two years, the effort eventually scaled to 36 countries by ISC's end.

The ISC addressed the second purpose through three main tasks:

- Equipping partners with IT staff with the necessary knowledge and skills, despite the fact that most organizations were small and lacked in-house capacity.
- Identifying IT-capable Local Implementers who–like ISC's Digital Security Specialist –could work with Local Partners and train them in ISC protocols (assessing organizations, cybersecurity threat model and solutions for vulnerabilities), and dispense microgrants to cover the cost of convenings, travel, hardware, and software, among other things.
- Encouraging, when and where possible, Digital Security Specialists and Local Implementers to set up or partner with a local NGO in order to seek financing from other sources, such as OSF, the NED or small grants programs administered by other Western-country embassies so as to continue to provide cybersecurity support to Local Partners.

As a result of this model, ISC Digital Security Specialist were able to train Local Implementers. In countries where the ISC has already exited, the takeaway has been that the model worked, though the pool of local digital security experts has tended to degrade each year as Local Partner staff changes, thus gradually losing touch with those who were helping with cybersecurity as local experts move on to other jobs.

Country Assessments

At the inception of the ISC, cyber threats differed greatly from country to country. ISC's staff invested considerable time and effort identifying what kind of help was needed in each geography, including establishing a country assessment framework to analyze and rank cybersecurity threats on a number of axes, and assign resources for solutions to the highest priority cybersecurity defenses.

As the decade unfolded, the country assessments became less important as the playing field leveled out, both in terms of threats and defenses. All of ISC's Local Partners, regardless of country, began to see and experience attacks that had previously been specific to a geographic region. Thanks to improved defensive tools, it became much easier to apply a standard set of sufficient defenses for all Local Partners. Toward the end of the ISC, the value of building country-by-country threat models decreased, and the team stopped investing in maintaining the accuracy of the country assessments.

Capacity Assessment

Because successful cybersecurity depends not only on adopting defensive solutions but also on the end user's trust in the person providing assistance, the ISC's Digital Security Specialists were chosen in part based on the strength of their relationships with in-country activists, NGOs, journalists and the wider media.

The differences among these specialists were an asset to the ISC and meant no single cybersecurity auditing mechanism was forced upon staff. In

general, each ISC cybersecurity assessment began—partly for pedagogical purposes—with learning from the Local Partner what they cared about defending: the confidentiality and integrity of their data bases and organizational records, external communication, files, and metadata (e.g., not just the content of a journalist's communication with a source, but the source's identity).

Much of the Digital Security Specialists' work was spent encouraging a Local Partner to shift their focus from solving a specific problem ("*I lost control of my account, how do I get it back?*") to setting up a broader defensive solution (enabling 2FA to prevent an attacker from stealing an account). Because many cybersecurity problems were already known, the capacity assessment process created key opportunities, such as focusing on problems not yet solved and getting those problems fixed, and building capacity among Local Partners to improve their ability to identify vulnerabilities and thus enabling them to remediate future threats on their own.

ISC's Digital Security Specialists also worked with Local Partners on implementing a set of mandatory core defenses, and assessed needs across a set of varied solutions. The optional defensive solutions had both costs and marginal value, and evaluating whether they were worth investing in *a priori* (as opposed to waiting until an attacker's tools, tactics, and procedures justified the investment) was part of ISC's approach. This frequently placed ISC's Digital Security Specialists in the uncomfortable position of discouraging a Local Partner from using a certain tool (Tor, Deflect, or a VPN) in order to redirect their focus toward getting the basics in place (e.g., eliminating pirate Windows or enabling 2FA on accounts).

ISC supported Local Partners with a core set of requisite cybersecurity fixes, and also offering additional, optional solutions based on their priorities:

- For **online anonymity**, teach a journalist to use Tor, an anonymity-providing browser.
- If an adversary wants to prevent netizens from seeing an NGO's web site content, get them to use Deflect, Galileo, or Shield to **protect from distributed denial-of-service attack**.
- When facing online cybercensorship, such as an inability to access online resources because of **ISP or government-instituted blocking**, get activists or NGOs access to VPN services.

Cybersecurity Assistance and Workshops

Earlier cybersecurity projects offered workshops, and Counterpart found that many civil society organizations and actors were conditioned to expect this form of help from projects like the ISC. But the ISC's genesis was predicated on the need to move beyond teaching, particularly when what was taught was difficult and disruptive for the trainee to operationalize (for example, a USD 200 cost for a software license is a barrier to entry for replacing pirate software) or implement.

The relationship between the ISC's Digital Security Specialists and Local Partners who were supported by them proved a critical piece of the behavior change puzzle. The ISC held hundreds of cybersecurity workshops that were instrumental to achieving goals, but the workshops were not the primary metric for measuring results. And though the first interaction with the ISC often started in a workshop, most of the hard work took place during one-on-one engagements between Digital Security Specialists and Local Partner staff to assess the degree to which core fixes were adopted to remediate any gaps.

The ISC applied a simple implementation model in each country with small adaptations over the years. The engagement process began with an assessment of a country's cybersecurity threats and the Local Partner's cyberinsecurities, and quickly moved to building both capacity and trust with Local Partners. Once the relationship was established through frequent phone calls, emails, instant messaging, and, eventually, office visits, ISC's Digital Security Specialists began cybersecurity assistance and mentorship.

1 **Assess**
vulnerabilities & needs of local partners

2 **Plan & Change**
technology & behavior changes of local partners

3 **Mentor & Assist**
face-to-face mentoring, assisting, fixing

Training of Trainer Model

In addition to remediating cyberinsecurity for Local Partners' staff, ISC Digital Security Specialists worked to build capacity among other IT specialists in-country who could be brought up to speed on cybersecurity issues that the ISC identified as high-priority, educated on the simplest and most effective solutions to mitigate those problems, trained in a Training of Trainers (ToT) workshop to encourage end-users to adopt solutions, and ultimately connected with other Local Partners in order to become their in-house or readily on-call cybersecurity specialists (also known as Local Implementers). This model's utility varied widely depending on whether appropriate Local Implementers could be found and trust between them and Local Partners could be established, as well as on how motivated they were to assume the role. The ISC's Regional Managers made resources available to Local Implementers via microgrants, which helped finance out-of-pocket costs for cybersecurity support and assistance to Local Partners.

Training of Trainers Workshop

Network of local cybersecurity experts continue and expand digital security support in local communities

Customize the Training of Trainers Workshop

1. **Teach the ISC's Top Risks & Threats**
2. **Digital Hygiene**

Security of Endpoints
Software licensed, updated, patched, upgraded

Security of Accounts
2-Factor Authentication & Password Manager

Security of Data at Rest
Encryption (BitLocker, File Vault 2)

Security of Data in Transit
Encrypting messengers for IM & VoIP (replace POTS/SMS)

Security of Access
DDOS-defend your website and cyber-circumvention (proxy client, VPN)

3. **Technology Demos**
   Companies & tech developers demo tools
4. **Presentations & Feedback**
   Present & demo a Digital Hygiene training topic

Sustainability Through the Building of Local Capacity

If the ideal long-term solution of ISC's Local Partners taking responsibility for their own cybersecurity is perhaps optimistic because staff are unlikely to possess the requisite technical knowledge or are unwilling to accept the help they need to pay for it themselves, the need to support civil society actors is too high-priority for the US to adopt a "*let fail those developing-country independent media and rights defenders who do not prioritize cybersecurity defense*" attitude. Looking ahead, one option might be to support a local NGO to be able to provide ongoing support akin to that given by the ISC and its Digital Security Specialists.

The ISC did, in fact, envision this approach, and strived to either find a local NGO willing to take on this responsibility, or encouraged the formation of such an organization. Counterpart's experience with this aspirational model is mixed. On the one hand, the ISC's Digital Security Specialists tend to be (relatively) highly qualified. Upon finishing their engagement with us, they were generally more interested in and often able to find a better job, one with more stability and better remuneration than that offered by an NGO. When Counterpart sought to hire an NGO professional, it proved significantly more difficult to find someone with sufficient technical qualifications. When such a person was identified, tasking them with protecting civil society actors was a risky endeavor.

That said, ISC had success with this vision in two countries. Digital Security Specialists, with the ISC's support, created the Digital Society of Zimbabwe and the Digital Security Lab in Ukraine, both of which are still in existence. **Digital Security Lab** has had moderate success finding financing to continue its work thanks to the continued interest of a handful of donors interested in helping Ukraine stave off the face Russia's active campaign of disinformation, incivility, instability, conflict, and dissolution of democracy-seeking states in its neighborhood. Lacking a geo-strategic competitor as a neighbor, **Digital Society of Zimbabwe's** path has been rockier. Without donors willing to support its domestic work, it has turned to providing cybersecurity support to South African Local Partners and rebranded itself **Digital Society of Africa**.

Cyber Security Community Building

Events and Conferences

ISC's Digital Security Specialists were often asked to participate in conferences, speak as a guest lecturer, or give a talk or convene a workshop for other USAID programs. This was happily done, not with the expectation that it would lead to the adoption of cybersecurity solutions or behavior change on the part of civil society actors, but because it helped solidify the Digital Security Specialist's standing in the community. Having social capital meant that Local Partners were more likely to heed their advice about compliance with core cybersecurity defenses and principles.

Over its nine years, the ISC sent hundreds of participants, including ISC staff, Local Partners, and beneficiaries, to other internet freedom events, including RightsCon, the Internet Freedom Forum , the United Nation's (more or less) annual Internet Governance Forum, and related regional gatherings such as Bread & Net in Beirut and the Forum on Internet Freedom in Africa, all of which proved invaluable points of intersection to make connections, discuss problems, debate solutions, hatch plots, develop coalitions, and renew commitments to adherence to good governance.

Annual Global Workshop

At the ISC's launch, Counterpart's objectives included improving information-sharing among the community of aid providers supporting developing-world civil society's cybersecurity. Under this objective, the main activity vector was conducting an ISC Annual Global Workshop for 100-200 practitioners. Most of these events were convened in Washington, DC, though the last one was held in 2019 in Nairobi, Kenya.

Over the eight years the workshops were held, they evolved from more traditional panel presentations to more interactive formats, including speed geeking (where participants engage in brief interactions with a number of experts), an exhibition offering a more relaxed opportunity for participants to learn about new cybersecurity tools, self-guided discussion circles, rotating groups exploring tech demos, and facilitated exercises to generate

solutions to regional issues.

In addition to cybersecurity-as-aid providers and tool developers, ISC workshops invariably attracted tech companies interested in getting feedback on resources that could help strengthen developing-world civil society and governments, yet not be abused by authoritarian states. Representatives from Microsoft, Google, Facebook, and Twitter participated regularly, as well as (then) smaller companies like Cloudflare and SpiderOak.

Several years after its inception, other organizations in the civil society and technology space began convening similar annual events—most notably, the Internet Freedom Festival and RightsCon. Eventually, the need for the ISC to contribute to this space diminished, and USAID approved Counterpart's recommendation to discontinue the Annual Workshop after 2019.

Locally Created Resources and Tools

The first decade of the 21st century was a golden age for coders to conceive and create tools that mitigated cybersecurity vulnerabilities. And although each tool was met with outpourings of enthusiasm, most did not provide as much utility as hoped. Often challenging to use, the tools were difficult to maintain, incompatible with some new use case, non-interoperable with other tools, and not easily adapted into additional languages. An understanding of these limitations, combined with the evolution of the US Government's internet freedom funding for tools migrating to the Open Technology Foundation (created after the launch of the ISC), resulted in the ISC providing less support for tool development over the years.

Instead, most of ISC's support for tool development in later years funded improvements to existing tools that had already proved effective for its Local Partners. For example, many of them used WordPress as the content management system to create, manage, and deliver their website's content to visitors. Thus, Counterpart assented to a request for financing submitted to by a pair of Latin American coders to produce an online site security probe for WordPress that ISC staff and Local Partners could use to conduct a routine check-ups to identify the most common errors that might allow an attacker to compromise a WordPress-hosted site's security or degrade its performance.

Technology Development

In the later stages of the ISC, Counterpart chose to allocate a small portion of its resources toward trying to solve four recurrent problems for which no off-the-shelf solution could be found.

Digital Security Specialist (DSS) Helper

The first technology problem ISC set about solving was to provide its Digital Security Specialists with a tool they could use to track their many Local Partners' and individual staff's devices, potential cybersecurity problems, and status updates. If, on average, an ISC Digital Security Specialist set out to provide cybersecurity support to fifty Local Partners, each of whom had an average of ten staffers who, in turn, each suffered from several of ISC's core cyberinsecurities, then each Digital Security Specialist's mission could potentially entail evaluating and resolving ~7,500 problems.

Using Microsoft PowerApps, Counterpart addressed this issue by developing the **DSS Helper** application. Built by an in-house developer, **DSS Helper** is a Counterpart-hosted database, which ISC Digital Security Specialists were able to access via a customized web page visible in a PC's browser (easiest for initial data entry), as well as an application compatible with both Android and iOS smartphones and tablets (easiest for updating Local Partner staff updates while in the field). Because the **DSS Helper** initiative arose relatively late in ISC's life, it was only adopted by ISC's last dozen or so Digital Security Specialists, though it proved useful for them as part of their auditing process helping to identify Local Partner staffers in their care, the initial status of each of the ISC's core cyberinsecurities, and the Digital Security Specialist's progress toward ensuring all problems were solved. It also provided ISC management with visibility into which problems were most prevalent and where, and how many problems were solved by and for whom.

As **DSS Helper** is built around an in-house Windows SharePoint Server backend, and uses PowerApps (part of the Microsoft 365 E3 license that Counterpart buys for staff use), it is not easily released publicly for others to copy/use, although of course ISC Digital Security Specialists carry with

them knowledge of how **DSS Helper** works should they wish to replicate it in other settings.

CertainTLS

The second problem ISC addressed was prompted by the Kazakhstan government's August 2019 move to require nearly one million of its netizens to download and install a new trusted root certificate in order to connect to ~250 foreign web sites. Thus, whoever owned the certificate (e.g., presumably Kazakhstan's law enforcement agency) could silently intercept and / or compromise connections to Facebook, Gmail, and Twitter – a stunning example of state-imposed cybersurveillance. In response, Counterpart imagined, defined, contracted, and built **CertainTLS**, a tool enabling anyone using Windows, Android, macOS, or iOS to see which root certs their device is trusting, learn which of those root certs should be considered untrustworthy, and choose to explicitly distrust a dubious root cert within the constraints of each operating system.

CertainTLS functions as advertised, so aside from having been deployed for ISC Digital Security Specialists to use when auditing Local Partners' devices, information about its availability and use is seeded through the cybersecurity community via personal contacts and limited internet-search advertising.

CertainTLS has its own domain which redirects to its GitHub page where all its code is available open source. For Android phones, **CertainTLS** is available in the Google Play application store. To date, Apple has not yet allowed **CertainTLS** to be included in the App Store that supports iOS devices – likely on account of it using undocumented Apple APIs to accomplish its goal. For a different reason, Microsoft has not yet allowed **CertainTLS** into the Microsoft store, which would simplify its installation in Windows. Efforts are ongoing to resolve both application store issues.

MiddleMonster

The third problem Counterpart tried to address involved attempting to invent a more-effective real-life example of cyberinsecurity to convince a netizen to take cybersecurity advice seriously. Specifically, we wanted an off-the-shelf capability in hardware and / or software to be able to compromise Facebook or Gmail logins using an innocuous mechanism that did not install anything malicious to use during a cybersecurity workshop in order to demonstrate the importance of adding 2FA in addition to a strong password to online account security.

The ISC eventually code-named this project **MiddleMonster**. The coder contracted to build this solution only achieved ~70% of the goal due to effects of the COVID-19 pandemic and other related factors. The code is available open-sourced on GitHub so work can continue after ISC ends.

FixPanel

ISC's fourth self-generated technology project involved an attempt to create a software agent akin to a classic intrusion detection system, which could be installed on a staffer's devices to periodically check a specific number of basic cybersecurity parameters such as software updates, whether data at rest were encrypted, whether device access required authentication, as well as to call home to an ISC's Digital Security Specialist if there was a problem. The idea was to enable Digital Security Specialists to keep an eye on whether key cybersecurity settings were correctly and safely set on staff devices used by ISC Local Partners.

ISC eventually code-named this project **FixPanel**. The coder with whom Counterpart contracted achieved ~ 75% of the goal due to effects of the COVID-19 pandemic and other related factors. The code is available open-sourced on GitHub so that work can continue after the ISC project ends. **FixPanel's** coder has reported that several others others have contacted them expressing interest in forking.

Investment in Technology

In 2011, smartphones were young and rare and market penetration limited. There were no easy-to-use secure online communication methods, and one unit of the world's first cryptocurrency was valued at USD 2 (by comparison one Bitcoin is currently valued at ~USD 30,000). The OTF, which later became the US Government's main method of financing the technology side of internet freedom, had not yet been born. Consequently, USAID's original objectives called for the ISC to disburse subawards to finance the development or deployment of select cybersecurity-supporting technologies.

"Support cybersecurity" was rather broad, though, and the ISC instead chose to call for grant proposals to solve cybersecurity problems specifically faced by its Local Partners. The resulting grants supported the (1) technical testing of existing tools; (2) linguistic translation of an existing software interface, documentation, or training material; (3) creation of product documentation or training materials; and (4) the customization or improvement of existing tools. The focus of funding was thus on improving existing tools rather than developing new ones. During the duration of the project, ISC made 26 technology support grants.

Technology Support Grants

2013

iilab
Open Integrity Index

Open Integrity Index enables users to make sophisticated decisions about the tools they use for privacy and communications without requiring a high-level security engineering background. The project improved access to material on digital security principles in languages other than English. More information can be found at https://openintegrity.org and https://iilab.org.

radicalDESIGNS
Ethersheet

Ethersheet is an open-source spreadsheet, which makes it easy for groups of people to work securely at the same time. Ethersheet supports anonymity of the end-users by storing no personally identifiable information.

Intevation & g10 Code
Gpg4win

Gpg4win's open-source software was improved so that more users can benefit from its strong email and file crypto operations. It also produced new Gpg4win installers that fixed some known issues while being more compatible with modern versions of Outlook and Windows.

Small World News
StoryMaker

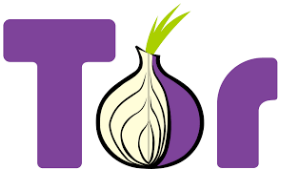
StoryMaker added important privacy features and improved the design of StoryMaker. It directly integrated the Guardian Project's work on the redaction filter for ffmpeg (first seen in the ObscuraCam app) to protect anyone appearing in a story who wishes to remain anonymous.

HacDC
Project Byzantium

Project Byzantium developed a live distribution of Linux for rapidly and easily constructing ad-hoc wireless mesh networks during emergencies.

The Guardian Project
Bazaar

Bazaar spearheaded development of an open-source repository and accompanying application (the "Bazaar") for the promotion and dissemination of software promoting privacy, anonymity, circumvention, and steganography.



Tor Project
Stegotorus

Stegotorus is a tool designed to disguise Tor traffic to resemble an uncensored protocol, such as HTTP. The project improved the tool to make it more reliable, as well as approachable for non-technical users.

CAP Solutions
Tor Browser Bundle (TBB)

CAP Solutions implemented an enhanced design of a new Tor Browser Bundle (TBB) user interface. The group conducted individual usability testing sessions with a variety of technical and nontechnical users following a simple set of instructions to install, configure, and utilize TBB with the revised interface.

WITNESS
InformaCam

InformaCam is a mobile application seeking to address issues of authentication for digital media. The application turns on a user's mobile device sensors to track GPS and directionality, as well nearby devices to enable the user to enhance information about the context surrounding the capture of images and videos.

Brave New Software
Lantern

Lantern focused on the ability to access blocked Internet sites through a highly usable tool that is both fast and resistant to blocking attempts. Lantern uses a peer-to-peer trust network at its core, relying on trusted users being invited to the system both inside and outside of countries with government-sponsored internet filtering.

Technische Universität München (TUM), Germany
OONI

OONI is a tool used to automatically detect and locate man-in-the-middle attacks that was ultimately extended to include more hosts in different countries from which to conduct the tracerouting.

Bytes for All Bytes for All

Bytes for All Bytes for All executed translation of select training material focused on cybercircumventing censorship and general information security to Urdu language for its stakeholders in Pakistan.

2016

Small World News
Updated Documentation and Use Cases for CameraV

Subgraph
Updated its OS Documentation

The Tor Project
Updated its Mobile "Security Slider" and Community Usability

2018

Center for the Cultivation of Technology (CCT)
Expanded the capability of TAILS to be installs on macOS, Windows, and on UEFI computers

Digital Security Lab Ukraine
Updated its online resource of localized digital security knowledge in Ukraine

Sublime Software Ltd
Updated the application to allow Right-to-Left Language Support for Briar, its open-source messaging application

2019

TAILS
Adapted its Linux distro system into a USB Image format

Guardian Project
Completed an integrated workflow between Google Play, F-Droid, Weblate, and application developers without requiring the use of extra XLIFF files

Sublime Software Ltd
Conducted user testing of right-to-left language support and validation of language with native Arabic and Farsi speakers for the peer-to-peer encrypted messaging application, Briar. The testers identified some smaller visual issues that Briar resolved and published a new version of the application in Google Play Store and F-Droid

2020

GreatFire
Rewrote its code to better integrate with global censorship-testing websites and data science tools. GreatFire's Analyzer tool tests and records information on which foreign websites are being blocked by the Chinese firewall

TAILS
An open-source OS that can be booted from a USB thumb drive. ISC's grant helped developers refresh their nearly ten-year-old website descriptions and tutorials in order to expand the OS's accessibility

Nothing2Hide
Translated two Totem cybersecurity courses from English into French to support remote training of journalists and activists in Francophone Africa. The team procured machine learning software to help translate the training material for Massive Online Open Course entitled *Choosing a Secure Messaging App* and *How the Internet Works*

Sublime Software Ltd
Improved Briar's Tor, Wi-Fi, and Bluetooth connectivity by adding a feature for users to enable or disable connections from their interface. Developers also added support for IPv6 link-local addresses thereby making it easier for devices using the application to connect to each other when joining a new Wi-Fi network

Guardian Project
Improved translation workflow for their open-source applications and libraries. GP's core application suite (Orbot, Orweb, ChatSecure, Courier, FDroid) provides basic privacy and security capabilities for the common activities of browsing, messaging, and installing mobile applications

Cyber Policy Support

Six years after the launch of the ISC, USAID asked Counterpart to add a policy component to the ISC's objectives. In response, Counterpart added IGIF, catalyzing ISC sub-awards to over a dozen local NGOs in developing countries in support of pro-cyberliberty policy.

Initial projects eased the ISC into cyberpolicy. Subawards supported research that could be used by policy advocates to demonstrate to policymakers the importance of increased online freedom. Resources were also used to finance public information campaigns, which informed citizens of the importance of defending and promoting digital rights.

During the ISC's final year of implementation, the project renamed this work IFPA, and issued a global APS calling for proposals to support government-facing advocacy. Of the 50 applications the IFPA APS received, ISC made subawards to ten local NGOs in as many countries.

All IFPA work focused on domestic cyber policy in developing countries: Some subawardees focused their work on the legislative branch advocating for the adoption or amendment of a specific law; some focused their efforts on the executive branch advocating for specific regulatory changes or enforcement; some focused on the judiciary advocating for the training of judges or conducting strategic litigation; and the rest focused on privacy, surveillance, or cybercrime.

ISC augmented IFPA's financial support for local policy advocacy with mentoring for subawardees. ISC's plan to conduct in-country policy advocacy training launched with workshops in Zambia and Zimbabwe, but was delayed and ultimately cancelled due to the COVID-19 pandemic. Instead, our two mentors—one from the US's premier cyberliberty advocacy NGO, the Center for Democracy and Technology, and the other from the UK's analog, Open Rights Group—divided the ten subawardees between them and reached out regularly via e-mail, instant-messaging, VoIP, and video to provide legal, advocacy, research, and communications advice, as well as oversight to keep advocacy efforts on track. The most aggressive advocates leveraged a silver lining in the COVID-19 pandemic by successfully reaching policymakers who were less busy than usual because of suspended parliamentary processes.

ISC IFPA subawardees deployed all the usual tools in the advocate's toolbox, from identifying government champions, coalition-building with leaders in both business and academia, reaching out to security agencies to find common ground, to collaborating with international media groups to influence domestic policy.

IFPA-like support for policy advocacy not only raised the visibility of key issues, advanced pro-freedom policy, and increased local civil society advocacy capability, but also drew new players into the pro-good-government field who, per Counterpart's past experience, will likely end up becoming MPs, regulators, or presidential advisors.

Internet Freedom Landscape

If the first decade of the 2000s was generally one of increasing internet freedom, the second decade has witnessed a distinct reversal.

Some countries – Tunisia, Myanmar, and Yemen – stopped cybercensoring, while others – notably Egypt and Russia – began imposing restrictions. The three largest cyber censors – China, Iran, and Vietnam – worked hard to maintain national firewalls, although the pro-internet-freedom community has generally held its own, providing ever-more-sophisticated cybercircumvention tools.

While good-governance advocates are right to fear security services, Counterpart generally prefers government to codify cybercrime law (even if defined more broadly than we would like) than for the absence of law to be abused by law enforcement agencies, which assert that anything not permitted to a user is forbidden while anything not forbidden for a law enforcement officer is permitted. In the same vein, good-governance activists can encourage policymakers toward acceding to the Budapest Convention on Cybercrime, which dangles the carrot of an effective ability to subpoena data from other signatory countries' tech companies—the prize, of course, being access to signatory US's Google, Microsoft, and Facebook et al. In

exchange, signatory countries must agree to adopt and implement strong human rights protections preventing law enforcement's abuse of cyberdata to persecute activists without due process.

A markedly positive trend on the cyber policy front is the increasing number of donors aware of the problem of threats to cyberfreedom by restrictive governmental policy who are prepared to step up and help finance solutions. In particular, the Ford Foundation and Omidyar's Luminate have provided much-needed resources to local internet freedom advocacy organizations, including the ten IFPA subawardees supported by ISC.

Internet freedom advocates in the 2010s continued to play to their strength, quickly identifying emerging, cutting-edge issues and working with developing-country policymakers to adopt netizen-friendly policies before actors with vested interests could put in place policies that would thwart pro-consumer regulation – a recent example of the former being PDP. Many countries still lack explicit policies controlling data collection, retention, and use. Putting in place a citizen-friendly regulatory environment is far easier before domestic data brokers gain power by profiting from tracking a user's every move, collating data from different sources, and on-selling it to buyers who want to micro-target netizen for commercial or political purposes.

Design Principles for Internet Freedom Support

ISC's IFPA work aimed to build upon the experience donor-supported internet freedom efforts had gained – initially with the Global Internet Policy Initiative; then with several DRL Internet Freedom grants to Internews; and ultimately expanding beyond conventional efforts with the work of Article 19 and Global Partners Digital, as well as consultation with other donors, such as Open Society Foundations, Ford Foundation, and Luminate.

Overall, ISC sought to support pro-cyberliberty policy advocacy work as follows:

- **Engaging local groups** rather than donor-funded project employees.
- Working directly with **in-country teams**, as opposed to intermediaries.
- Working **consistently 24/7** as opposed to sporadic intervals.
- **Supporting government-facing advocacy**, rather than public information campaigns or workshops for students or journalists.
- **Supporting grass-roots advocacy**, instead of research or publishing.
- **Focusing on domestic issues** in lieu of international sessions at the ITU or ICANN.
- **Encouraging specific law-based remedies** above digital bill of rights statements.
- **Supporting internet freedom issues** that directly affect netizens' ability to freely and securely communicate, organize, and conduct transactions.

Bearing in mind that not all advocacy work in this field meets these high bars, ISC's IFPA activity was deployed to work toward achieving specific policy goals, as well as to encourage developing-country actors toward these indicators of quality and integrity.

Internet Governance and Internet Freedom:

2017–2019 Subawardees

During the ISC's first two years of cyber policy work, Counterpart made subawards to the following Local Implementers:

- Ukraine
- Zimbabwe
- Venezuela
- Sri Lanka

Ukraine

Human Rights Platform collaborated with **Digital Security Labs** to provide pro-internet-freedom litigation support for journalists, activists, and independent media. Initiatives included litigating when a government agency ordered a domestic website blocked by Ukrainian ISPs, as well as when it refused to make data available in an easily readable online format.

Having engaged stakeholders in various rounds of dialogue, **Internews Ukraine** was able to develop the Green Book, a practical handbook for Ukrainian government officials and legislators to use when drafting, adopting, or implementing internet freedom legislative initiatives.

Zimbabwe

MISA Zimbabwe actively participated in submitting recommendations for consideration during public consultation periods, as well as contributed to parliamentary hearings in favor of the following three pieces of legislation: *Access to Information and Protection of Privacy Act*, *Broadcasting Services Act*, and *Cybercrimes and Cybersecurity Bill*. Additionally, **MISA Zimbabwe** continues to organize the annual Internet Governance Workshop in Harare, which provides a platform for citizens to engage with myriad stakeholders, such as government, service providers, and CSOs working to promote internet freedom regionally, as well as in Zimbabwe.

Venezuela

Given Venezuela's authoritarian regime, **IPYS**' work focused on capacity-building and evidence-based research as opposed to promoting the adoption of progressive policies. For example, **IPYS** trained 25 journalists, as well as other activists in Barquisimeto, Caracas and Merida, to contribute to consistent nationwide monitoring of cyber censorship. Additionally, by deploying the *OONI Explorer* data repository tool to monitor and maintain records that supported policy advocacy driven research, **IPYS** emerged as one of the foremost organizations in Latin America reporting on the impact of internet censorship and digital rights violations. **IPYS's** report on cyber censorship, Intercortados, was chosen as one of the 40 best works (in a pool of 1,700 submissions) in the innovation category for the Gabriel Garcia Marquez (Gabo) subaward.

Sri Lanka

Perceptions and Experiences of Online Security and Privacy by Internet Users, a study undertaken by IGIF subawardee **LIRNEasia** measured the relative ease of internet access experienced by the country's citizens (disaggregated by age and gender). The study also looked at differing perceptions and expectations of privacy and security. **LIRNEasia's** study contributed to the ongoing research project to examine regional practices in Asia being conducted by Canada's International Development Research Center.

Internet Freedom Policy Advocacy

2020 Subawardees

In the final year of the project, ISC shifted its strategy from supporting civil society advocacy campaigns to one focused more on engaging policymakers. The decision was based on the assumption that the improvement of internet regulatory environments is largely accomplished through effective and balanced legislation. By engaging legislators and building their capacity to draft pro-cyberliberty laws, ISC determined that Local Implementers would have better success in advancing internet freedom.

To promote its agenda, ISC's IFPA team launched APS to assist Local Implementers on projects that:

- Empower civil society to counter restrictive internet laws; support policies to promote a free and open internet in targeted countries where the government has adopted, or is considering adopting, laws or policies that restrict online rights.
- Identify and support champions amongst government actors to help them steer the policy agenda.
- Provide expertise to domestic policymakers to encourage the adoption and implementation of data protection and privacy laws.
- Build coalitions with leading civil society actors, businesses, academics, and other influential members of society.
- Encourage accession to international internet-freedom-enhancing agreements, such as the Budapest Convention.
- Convene hearings and / or roundtable discussions on draft laws; and
- Work with media to catalyze broad support for internet-freedom-friendly policies.

The APS selection committee consisted of technical experts from the ISC, including the Chief of Party and Senior Officer for Policy Advocacy, who evaluated submissions in two rounds. In the first round, over 50 **Concept Notes** were received from 30 countries (Asia: 8; South America: 3; Europe & Caucasus: 5; Middle East: 1; Africa: 13). From this pool, ten were selected and provided with consolidated concept feedback to inform a full proposal submission. The selection committee then engaged applicants in a second round, the **Co-Creation** phase, in which submissions received more precise feedback and guidance on technical approaches and activities, budget revision, and alignment with APS scope and objectives. Applicants were encouraged to focus on direct, policy-focused activities to support advocacy efforts. The final subawardees, who came from ten different countries, proposed projects at different stages of the legislative process that engaged different arms of the government.

While each IPFA subawardee operated under unique legislative challenges, they all applied policy advocacy approaches that had been championed by experts from the Center for Democracy and Technology. ISC engaged experts to further mentor subawardees based on their decades of experience with tech policy, lobbying, and legislative efforts in the US and Europe.

COVID-19 was a major challenge faced by IFPA subawardees, many of whom had planned meetings with policymakers, as well as visits from international experts and other stakeholders. Video conferencing was utilized as an alternative for most face-to-face activities, however the adjournment of parliament in countries like Tanzania meant that many policymakers were not available for meetings in any format.

Internet Freedom Policy Advocacy Accomplishments

Depending on the legislative environment of each country, some IFPA subawardees focused on drafting new internet freedom laws, while others worked to analyze existing policies and their enforcement. Though they varied in terms of capacity and the tactics they employed, they all used consensus-driven policy engagements to analyze and understand their respective policy landscapes and identify champions in government, and collectively agreed on specific issues and opportunities to drive policy agendas and reforms.

The organizations supported with IFPA subawards, who have already made gains that bode well for the road ahead, continue to work on policy change goals that will take years to realize. IFPA subawardees produced 14 policy papers, 3 draft laws, and 8 positioning or monitoring papers, in addition to hosting 59 roundtables, online discussions, and one-on-one meetings with parliamentarians, judiciaries, and other stakeholders to advance cyberliberty agendas. In 2020, the Thomson Reuters Foundation honored **Fundamedios** (Ecuador) with the **TrustLaw Collaboration Award 2020** for its work drafting two new pieces of legislation, the *Personal Data Protection Act* and *Access to Public Information Act*.

Grandlex *Armenia*

Goal: Free and non-discriminatory access to the Internet

Tactics: Amend laws on Protection of Personal Data, Electronic Communication, and Code of Administrative Violations

Achievements: Drafted amendments to the country's Law on Electronic Communication ensuring net neutrality and personal data protection, which will be considered at the next National Assembly

Society for Media and Suitable Human-Communication Technique (SoMaSHTe) *Bangladesh*

Goal: Greater protection for social media communicators and online journalists

Tactics: Influence CSO support of digital media freedoms

Achievements: Published a shadow report, *Freedom of Online Expression in Bangladesh: Trends and Challenges*, which addressed commitments made by the state during the previous *Universal Periodic Review* (UPR) to revise its existing *Information and Communication Technology Act* (2006) and redrafted the *Digital Security Act* (2018) to ensure compliance with international freedom of expression standards

Fundamedios *Ecuador*

Goal: Development of an open and democratic Internet to fight corruption and consolidate democratic institutions

Tactics: Promote articles of consideration for the *Personal Data Protection Act* and *Access to Public Information Act*

Achievements: Drafted two new pieces of legislation, including the *Personal Data Protection Act* and the *Access to Public Information Act* that are currently under review by Ecuador's Council of Legislative Administration

Institute for Development of Freedom of Information (IDFI) *Georgia*

Goal: Safeguard digital freedoms through legislation

Tactics: Influence the parliamentary review process for the Law on Information Security bill

Achievements: Successfully advocated against the adoption of dangerous amendments to the country's *Law on Information Security* bill, which is no longer being considered by Parliament

ELSAM *Indonesia*

Goal: Digital safety and digital privacy is ensured for Internet users

Tactics: Promote a human rights framework within the country's cybersecurity bill

Achievements: Completed an alternative academic version of the country's cybersecurity bill and presented it to different stakeholder groups, including ministries, institutions, representatives from corporations, and CSOs

MISA Mozambique *Mozambique*

Goal: Ensure new Cybersecurity law adheres to international standards

Tactics: Engage with parliamentarians on a cybersecurity legal framework

Achievements: Drafted Mozambique's first *Cybersecurity and Data Protection* bill informed by leading internet freedom activists, academics, and politicians

Paradigm Initiative *Tanzania*

Goal: Protect citizen's data and internet freedom by law

Tactics: Form an advocacy coalition to enact a digital rights and freedom bill

Achievements: Produced a policy brief on the country's *Electronics and Postal Communications Act* (2018) and *Cybercrimes Act* (2015), which recommended the creation of a data protection law to close legal loopholes that put individual liberties at risk

Human Rights Platform (HRP) *Ukraine*

Goal: Ensure digital rights are considered when passing or enforcing legislation

Tactics: Define internet freedom to policymakers and the judiciary

Achievements: Finalized pro-freedom of expression amendments to Ukraine's Draft Law #2693-d governing the regulation of online media, video, and information sharing platforms after multiple rounds of input were submitted by policymakers, members of the judiciary, ISPs, the FreeNet Coalition, and other activists

Bloggers of Zambia *Zambia*

Goal: Encourage members of parliament to protect online rights and freedoms

Tactics: Build capacity of policymakers on international conventions

Achievements: Published a position paper in collaboration with local CSOs – *Key Cyber Legislation Impacting the Right to Freedom of Expression, Peaceful Assembly, and Association in Zambia* –whose recommendations were handed over to the Ministry of Transport and Communications

MISA Zimbabwe *Zimbabwe*

Goal: Encourage policymakers to adopt a strong, rights-based approach toward digital regulation

Tactics: Align *Cybersecurity and Data Protection Bill* with model law

Achievements: Published a policy brief for CSOs and policy guide for MPs on the country's recently gazetted *Cybersecurity and Data Protection Bill* that protects digital rights and freedoms

Spotlight on the DSS Helper Application

By year nine of the Project, ISC had supported more than 16,500 persons and 730 organizations across 36 countries to address widespread cybersecurity issues. By then, each Digital Security Specialist was supporting ~40 independent media platforms and civic organizations with an average of 10 staff or volunteers. Based on ISC's cybersecurity framework, which focused on solving 15 technical problems for every Local Partner staff member, Digital Security Specialists had a vast number of cyber security problems to solve. Measuring the success of this aspect of the project was a challenge, and presented ISC with the need to develop a system that could provide clarity on the impact of its work while organizing the efforts of the Digital Security Specialists. In the absence of an existing problem-tracking tool being readily available, ISC decided to develop something from scratch internally.

Collaborative Problem Solving

Counterpart HQ employed its Innovation Specialist from Program Quality and Learning (PQL) to lead the design of a new tool, starting with a **research and discovery** phase that included interviews with stakeholders likely to utilize either the tool or resulting data. Each discussion sought to answer the following three key questions:

- What information do you need to do your work?
- How do you currently organize the information you care about?
- What level of confidence do you have in cloud-based solutions for information storage, and what would need to be done to make you feel comfortable in using the software?

During the user analysis phase, the Innovation Specialist determined the following:

1. **Stakeholders focused on different cybersecurity problems.** The Chief of Party prioritized a set of 15 issues, while the Digital Security Specialists had varied concerns, depending on their operating environment and the needs of Local Partners.
2. **Users had different levels of confidence in cloud-based storage.** While some had confidence that online databases could be secured, others preferred to store data exclusively on an encrypted hard drive to which only they had access. Because the new tool would rely on cloud-based storage, this confidence gap would need to be addressed.
3. **Stakeholders cared about plans as well as problems.** The problems that security specialists addressed typically emerged through a process of assessment and action planning. While the design brief for the application was limited to tracking the status of problems, the assessment and action planning steps that preceded support to resolve problems would also need to be taken into account.

Additionally, the Innovation Specialist looked at how others had addressed similar challenges in the past with data collection tools like Microsoft Forms, Survey Monkey, Google Forms, and freemium CRM services like Hubspot. Microsoft PowerApps, which allows users to develop mobile and web applications using Microsoft Flow to manage tasks and SharePoint lists to store data, was a compelling option due to the team's lack of developer skills, small budget, and existing license.

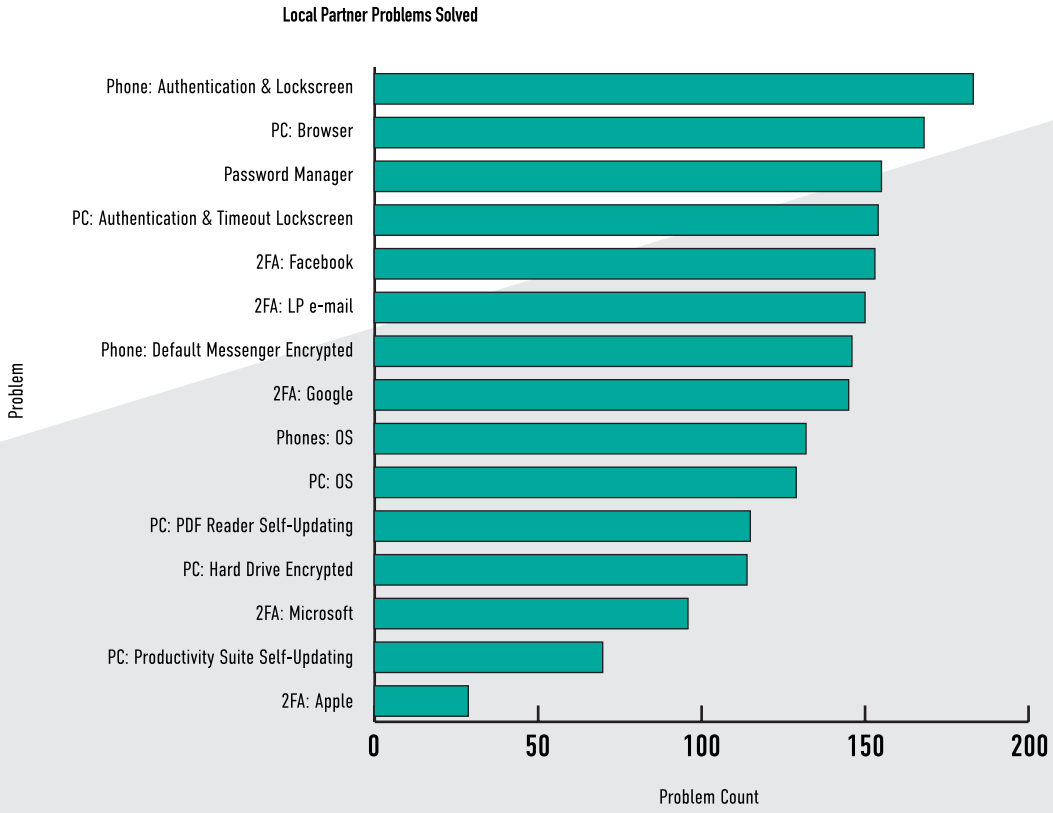
Innovation

The first version of the application was simplified to focus on 15 key issues deemed most critical to Local Partner safety. The efficacy and safety of using a cloud-based solution were addressed by elevating PowerApps's security features and limiting the granularity of data that would be gathered and tracked. Digital Security Specialists were instructed to continue as-is with their assessment and action planning tools.

During the design phase, the ISC chose PowerApps to run the user interface and a SharePoint list as the data storage service. This solution allowed Counterpart to create a simple, mobile-friendly way to input data while retaining a user-friendly method for viewing and manipulating information within a browser. The beta application was able to be rolled out in a few days to Regional Managers and Digital Security Specialists for review and feedback, who responded by highlighting features they enjoyed, as well as suggestions on how information might be more intuitively structured and what information might be left out for safety and streamlining. A final version of the application was utilized throughout the final two quarters of the project.

Impact

As Digital Security Specialists went about solving the ISC's 15 core cybersecurity problems, they used **DSS Helper** to record progress with each Local Partner staff member at the individual level. As a result, over 1,900 problems have been marked as solved since the application's adoption in July 2020.



Part Three: Program Learning and Monitoring & Evaluation

ISC Project's Evolving Theory of Change and Adaptations

Having originated from a congressional earmark to support and promote internet freedom, Counterpart worked to develop the ISC in a way that would defend the rights of activists and independent journalists in developing countries who faced constrained civic spaces and cybersecurity threats. The ISC's design was based on the underlying assumption that target beneficiaries were already being assisted with cybersecurity at workshops and through the use of training materials; it was the more long-term defense for these populations that remained elusive.

The vision was for ISC to more consistently mentor beneficiaries and build up local digital security expertise to mitigate cyber insecurity and the risks posed to in-country activists and advocacy groups. Five years after the ISC launched, a second main activity vector was added. Specifically, the ISC sought to promote internet freedom through the improvement of cyber policies, and catalyze governments to adopt a regulatory environment that would help maximize the potential of the internet to contribute to economic development and good governance.

ISC Project's Theory of Change

ISC's implementation strategies and activities shifted in accordance with evolving Local Partner needs and the sophistication of staff knowledge and skills.

1

In the first two years (FY2012-2013), the Theory of Change for the ISC focused on the following tenets:

- *If* the ISC conducts digital security training, *then* Local Partners will have increased cybersecurity
- *If* the ISC provides technical assistance and mentorship, *then* Local Partners will have increased resiliency
- *If* the ISC develops or deploys technologies tailored to local cybersecurity needs, *then* the use of digital security tools will increase among Local Partners

2

In 2014, ISC expanded the Theory of Change expanded to include:

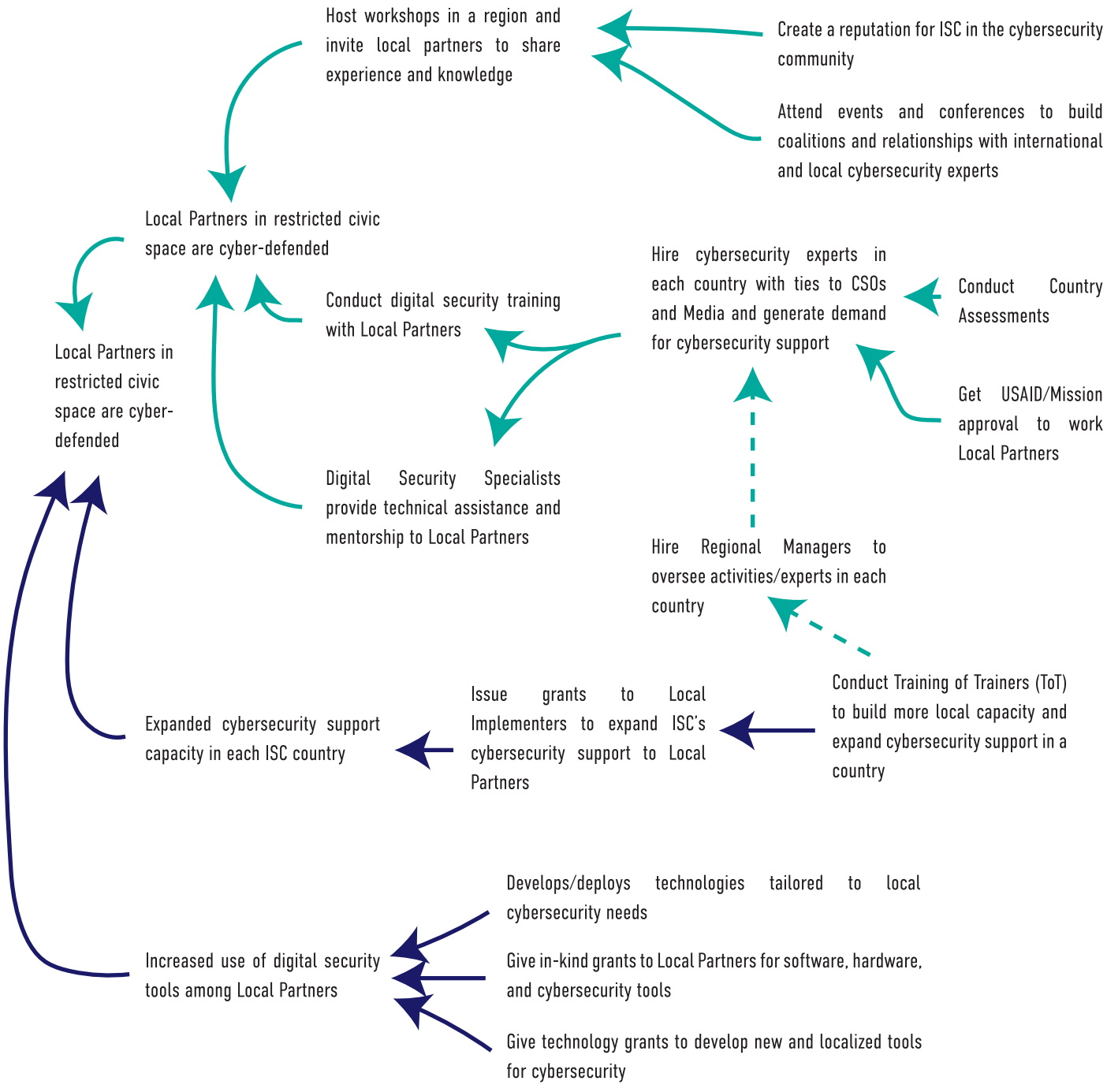
- *If* the ISC conducts Training of Trainers (ToT), *then* there will be a greater and more sustainable supply of local digital security experts
- *If* the ISC gives in-kind grants to Local Partners for hardware and software, *then* they can achieve and maintain cybersecurity

3

With the addition of internet freedom, the following was added to the Theory of Change:

- *If* the ISC issues grants for advocacy campaigns and research, *then* both understanding of internet freedom and the use of evidence-based research will increase
- *If* the ISC supports subawardees to participate in international conferences, *then* local research will be more widely shared, and learning from leading experts will increase
- *If* the ISC issues grants for domestic, government-facing advocacy on internet freedom issues, *then* new or amended internet freedom policies that protect citizens' digital rights will be enacted

Ultimately, ISC's approach to supporting internet freedom shifted from public-facing advocacy to government-facing advocacy, expanding in its last year from simply being aware of internet freedom issues to actively promoting policy changes and legislation to support and protect internet freedom and rights.



ISC Project FY2012 – 2013

During the initial years, the ISC was focused on networking within the cybersecurity community by attending relevant international and local events, and connecting with technologists. Throughout this early stage, the team was able to identify Local Partners, and regional cybersecurity experts and organizations, as well as tools with the potential to benefit the project. ISC staff also spent time and effort designing a research methodology to produce country assessment reports, which evaluated the suitability of countries for project implementation across three main vectors, including cybersurveillance, cyberattacks, and censorship. Numerical values were assigned to 15 possible threats, resulting in a composite index that prioritized countries in which to focus efforts. During the first two years, the ISC implemented activities with Local Partners in Azerbaijan, Belarus, Russia, Syria, Venezuela, and Zimbabwe and held two workshops in which Local Partners and tech experts participated.

ISC Project FY2014 – 2015

Throughout its middle years, the ISC expanded into new countries and increased support to technology developers. Local Digital Security Specialists were hired in Bangladesh, Bosnia and Herzegovina, Cambodia, Ecuador, Nicaragua, South Africa, Syria, Ukraine, and Venezuela as demand for ISC's services grew. In FY2014, Digital Security Specialists began conducting Training of Trainer (ToT) workshops to extend the reach and sustainability of ISC's efforts, as well as hosted numerous regional workshops to connect Local Partners and shore up the resiliency of ISC's network.

As local capacity grew, ISC began administering grants for individuals who completed the ToT to lead digital security trainings of their own for Local Partners. This expanded the reach of the ISC, allowing Digital Security Specialists to spend less time traveling to Local Partner offices, and more time providing mentorship to those under greatest threat.

ISC Project FY2016 – 2018

In FY2016, the ISC added a fourth objective designed to help Local Implementers supporting advocacy campaigns, research, and participation at international events. Resulting activities were designed to increase both government and civil society understanding of internet policy, as well as equip stakeholders with evidence-based research on why a free and open internet is beneficial. The ISC produced a comprehensive written assessment, *Internet Governance and Internet Freedom: Perspectives and Interventions*, which included the following four components:

1. Introduction to internet governance
2. Identification and review of major donor support and funding for internet governance activities
3. Identification of strategic activities to support
4. Recommendation of countries that could benefit from internet governance support

Sri Lanka, Ukraine, Venezuela, and Zimbabwe were identified as best suited, and Local Partners received subawards starting in FY2018. Subawardee organizations helped emerging activists push back against rights threatening policies in Ukraine and Zimbabwe, while ISC's partner in Sri Lanka conducted groundbreaking research on internet rights for women and Local Implementers in Venezuela published data on internet access that was used to justify the creation of a new Google censorship circumvention application.

ISC Project FY2019

With the growing network of Digital Security Specialists, ToT trainees, and Local Implementers, ISC hired regional managers for Africa and Latin America, Asia and The Balkans, and Eurasia to better oversee day-to-day activities in each country, and report back to HQ about critical in-country needs while at the same time dispensing technical advice to Digital Security Specialists and subawardees. Additionally, in FY2019 the ISC held its final Global Workshop, convening 84 participants from the international cybersecurity and cyber policy communities. ISC utilized this final conference as a learning event aimed at identifying cyber threats, as well as tactics used by authoritarian governments and methods for combatting them. A final session on regional horizon scanning helped regional groups design potential projects they could propose in ensuing years, while also affording regional managers and Digital Security Specialists an opportunity to provide feedback on the

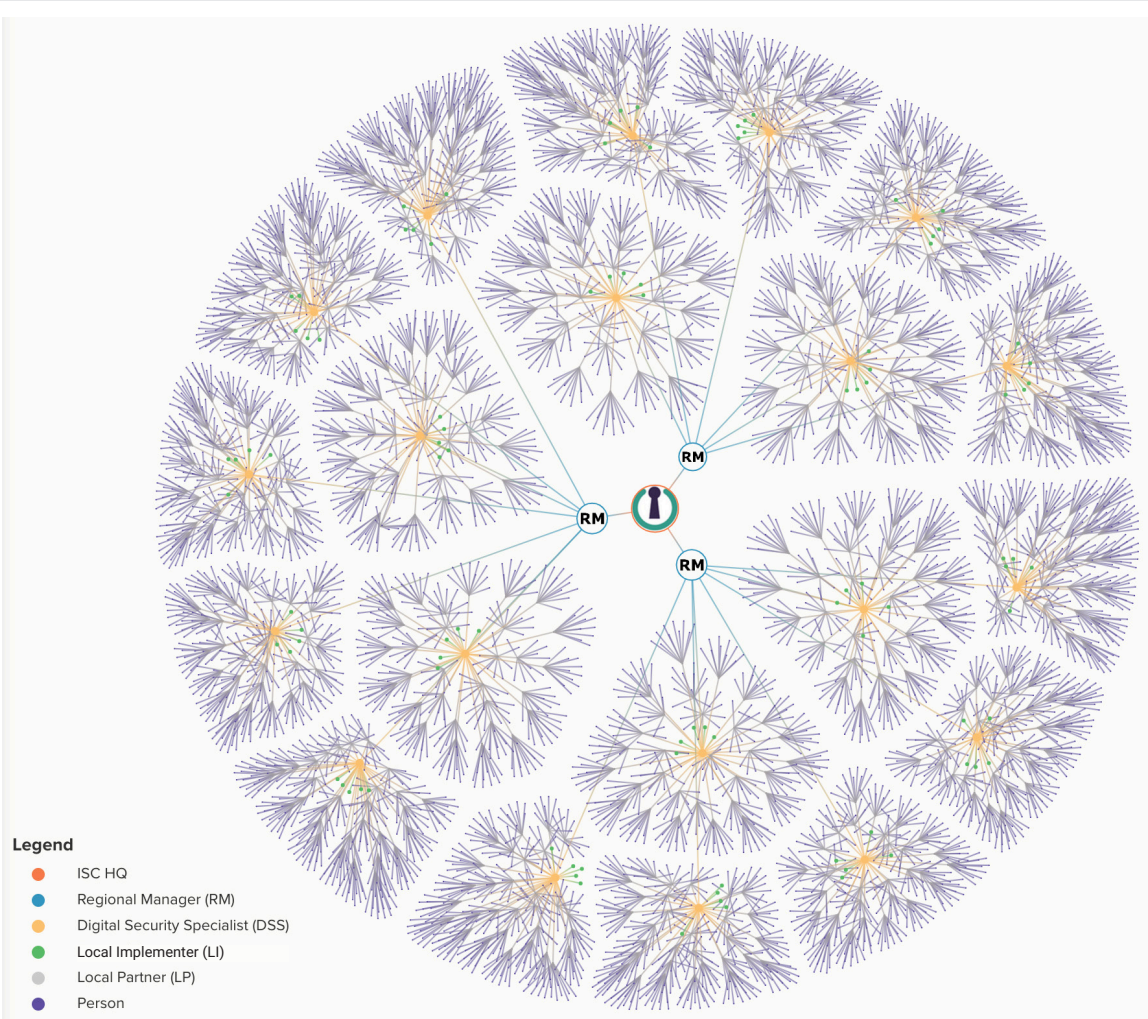
proposals and suggest potential funding opportunities.

ISC Project FY2020

In the final year of the ISC, a better understanding of the process of identifying potential additional countries and securing the cooperation of requisite in-country USAID missions, combined with increased funding and aggressive new leadership, enabled ISC to nearly triple the number of countries served by its Digital Security Specialists from eight to twenty-three. Three talented Regional Managers quickly launched fifteen new Digital Security Specialists, and the ISC was able to assist a record 3,711 individuals across 777 organizations.

In countries where the ISC had already been operating for a number of years, Digital Security Specialists shifted mostly to ToT workshops to build capacity among local experts who would – in turn – continue to assist Local Partners after the project ended. FY2020 also saw the greatest number of in-kind donations (USD 88,777), which helped equip Local Partners with software and hardware that will secure them for years to come.

Finally, the ISC decided to shift its internet freedom strategy in FY2020 to more actively engage policymakers to support the improvement of internet regulatory environments through legislation. By engaging this demographic group, and helping to build their capacity to draft pro-cyber liberty laws, the ISC also helped Local Implementers move the needle forward on internet freedom.



Monitoring & Evaluation and Decentralized Learning

At its peak, the ISC had Digital Security Specialists operating in 28 countries. The globally dispersed nature of the ISC meant that local experts actively worked to engage and secure partners to combat local cyber threats. During the Chief of Party (CoP) transition in FY2018-2019, it became difficult to capture high quality data at a useful frequency. Collecting performance indicator data was not a core competency for Digital Security Specialists and, as their workload increased, MEL became more challenging. Additionally, HQ staff often lacked first-hand knowledge of day-to-day activities due to the ISC's global scope and footprint.

To remedy these issues, Regional Manager positions were created to oversee the Digital Security Specialists and Counterpart's HQ Monitoring, Evaluation & Learning (MEL) team began training the ISC's Senior Program Officer on data collection and evaluations methods. Her promotion to become a full-time MEL Specialist dedicated to learning closed the gaps in ISC's knowledge, and decentralized the collection of key insights. Combined with a close working relationship with the Chief of Party and Regional Managers, these changes greatly improved the project's reporting capabilities, prioritized learning, and strengthened adaptive management practices.

New and longstanding Digital Security Specialists were required to participate in a MEL orientation, which clarified ISC's indicators and data sources needed for proper verification. The MEL Specialist also worked with HQ's MEL team to design a bi-weekly, semi-automated form to capture the stories and quarterly surveys of Digital Security Specialists to better assess broader trends in cybersecurity threats and methods for combatting them. The introduction of online tools and methods for MEL data was crucial to keeping the widespread ISC team on track to achieve output targets and collect impactful stories.

Increasing Investment in Monitoring, Evaluation & Learning

In previous years, the ISC's MEL activities were built around performance indicators, monitoring, and quarterly and annual reporting. However, as a result of daily interactions with Local Partners, coupled with constant monitoring of local cybersecurity environments, Digital Security Specialists developed unique insights that were not being shared because of ISC's infrequent and limited methods for capturing learning. Additionally, ISC leadership tended to rely on staff meetings, procurement processes, and grant close-out reporting as major sources of information for making management decisions about resources and operational needs.

To improve theISC's MEL capabilities, prioritize learning, and strengthen adaptive management practices, Counterpart HQ's PQL team began training the ISC's Senior Program Officer in Q42019 on data collection and evaluation methods, as well as Collaborating, Learning, and Adapting practices in Q4 of FY19. With support from the ISC's CoP and Deputy CoP, the Senior Program Officer was promoted to the role of full time MEL Specialist, and with a mandate to overhaul ISC's MEL procedures, they were able to increase the frequency and quality of reporting.

The newly appointed MEL Specialist strengthened the ISC's learning capabilities first by clarifying performance indicators – specifically data collection tools, methods, and data sources – as well as training and supporting ISC's Digital Security Specialists and IFPA Senior Program Officer to contribute to MEL activities. The MEL Specialist took the lead on ISC's data collection instruments, data verification and validation, and data analysis, and also engaged the Program Officers for each region on spot-checking the timeliness of data submitted by the Digital Security Specialists.

The MEL Specialist also worked with HQ's PQL team to introduce new MEL practices and tools that allowed the ISC to analyze and share qualitative insights necessary for data-driven storytelling, improve adaptive management, and deepen the technical evidence base, including:

- Organizing bi-weekly, semiautomated Microsoft Form data collection to capture details and insights from Digital Security Specialists about support given to Local Partners.
- Incorporating (virtual) MEL training for new Digital Security Specialists and refreshers for existing staff.
- Developing weekly Reflection Form completed online by Digital Security Specialists and Regional Managers to identify qualitative data and stories in a timely and easy manner.
- Weekly data talks with Digital Security Specialists to interpret and discuss form responses.
- Circulating a quarterly survey among Digital Security Specialists and Regional Managers to assess broad trends in cybersecurity threats and methods for combatting them, as well as specific threats faced by Local Partners and new cybersecurity tools and techniques adopted.
- Creating a participatory design process and user-testing and launching the **DSS Helper** application.
- Convening a *Capturing & Utilizing Data* workshop at the 2019 Global Workshop for ISC staff.
- Leading an Internal Data Quality Assessment with Counterpart's PQL team and the ISC MEL Specialist to identify and remediate gaps in data collection or analysis.
- Working with the IFPA Senior Program Officer to develop models for each of the IFPA FY2020 subawardees to help structure and streamline their reporting.
- Organizing key informant interviews and user-friendly report templates for subawardees.

Data Collection and Analysis

With more than 20 indicators covering four objectives, data collection was the responsibility of most of the ISC staff. A Knowledge Management Portal (KMP) designed by Counterpart for all GCSS projects utilized by ISC to store indicator data included important features like a Local Partner contact database, while activity forms for trainings and assessments facilitated the upload of information. The KMP also made it easy for users to adhere to required disaggregation, such as participant profiles (gender, age, marginalization or specialization) and organization profiles (NGO, media, marginalization or specialization). Lastly, by assigning separate roles for data capture, quality assurance, and data analysis, ISC was able to effectively and accurately analyze and report on indicators each quarter.

Data capture was completed primarily by Digital Security Specialists, who were responsible for uploading information about their trainings and assessments using the KMP activity forms. In instances where a ToT trainee or Local Implementer led a workshop on their own, the ISC took on the role of collecting that information and uploading it to the KMP. Required data sources, such as participant quizzes, sign-in sheets, agendas, and photos, were also stored on the KMP.

Quality assurance was completed by the ISC's HQ program assistants and program officers, who reviewed data sources and cross referenced them with operational and financial documents and receipts, such as hotel invoices and equipment rentals.

Data analysis was a task for technical leads, the Deputy CoP, and CoP until a fulltime MEL Specialist brought into the ISC. Data analysis took place bi-weekly, quarterly, annually, and as needed.

Evidence of Impact

In addition to the performance indicators, the ISC sought other methods for gathering information that could be utilized to demonstrate ISC impact.

Bi-weekly Form

Staff relied on bi-weekly story collection forms and follow up data discussions to identify interesting ISC success stories. The form included prompts for Digital Security Specialists to follow, such as changes in knowledge or awareness, changes in attitudes or behaviors, changes in participation in activities, changes in organizational sustainability, capacity-building and skills transfer, strengthening group commitment and perseverance, and building or acquiring new tools to benefit others.

After receiving form responses, the MEL Specialist often conducted follow up discussions with Digital Security Specialists to uncover more nuanced details regarding the stories and, afterward, published the findings. This information was then incorporated into a weekly newsletter that was distributed to relevant USAID Mission points of contact, as well as included in quarterly reports.

Grantee Closeout Surveys, Interviews, and Reports

Recipients of technology, Local Implementer, or IFPA subawards were required to submit final reports. To supplement this documentation, the ISC frequently designed surveys, interviews, and other reporting templates to assess lessons learned about grant implementation timelines, the types of support needed and provided, as well as potential future opportunities for collaboration.

Quarterly Surveys

In FY2019 and FY2020, the ISC's MEL specialist began designing and administering quarterly surveys to Regional Managers and Digital Security Specialists to collect contextual in-country information, including increased or new cybersecurity threats, political updates and news about changing legislative landscapes, as well as what – if any – assistance was being organized for specialized or marginalized groups. These insights were also included in quarterly reports, and used to formulate regional discussion questions.

The DSS Helper Application

Throughout the final year, ISC staff utilized the internally designed DSS Helper to record the number of digital security problems solved at the individual level. While the KMP was adequate for storing training data, it was not able to capture the hands-on fixing that Digital Security Specialists completed every day, such as encrypting hard drives, setting up secure networks, installing or updating software, and more. By being able to see, at a glance, which high priority problems remained unsolved among Local Partners, Digital Security Specialists could more easily update their assessments and plan assistances accordingly.

Results and Performance Indicator Analysis

Throughout the life of the ISC, 16 out of 20 performance indicator targets were either met or exceeded. The total number of individuals trained on cybersecurity basics reached **9,852 persons, 53 percent** of whom were female, exceeding the gender target by 3 percent. A further **1,487** local organizations were mentored by Digital Security Specialists and provided with over **USD 200,000** worth of hardware and software via in-kind donations.

The ISC's sustainability model was similarly successful, with ToT trainees extending the reach of the ISC to an additional **5,140 persons**, nearly double the target. **41 regional workshops**, **8 global conferences**, and **9 exchange visits** with technology partners helped to strengthen the inclusion of Local Partners with the international cybersecurity community, and facilitated dialogue between western developers and emerging markets advocates and policymakers.

Despite the fact the ISC had fewer years of to implement its programs and achieve its internet freedom goals, ISC succeeded in surpassing four of its six indicator targets. Subawardee organizations, who received support and expert technical assistance from the ISC, published **14 policy papers**, drafted **3 new cyberliberty laws**, and developed **8 judicial monitoring reports**. Over **60 roundtable discussions** and consultations with policymakers were also led by IFPA subawardees. Each organization played a vital role in advancing cyber liberty legislation across **12 countries**.

Evolution of Performance Indicators

The ISC modified indicators and recalibrated targets on an annual basis, and recorded these changes within the Annual Work Plans that were sent to the Agreement Officer's Representative. Initial indicators focused on country assessments and network building and, later, on training and workshop-based targets. This shift reflected a linear progression for the ISC, which initially focused on building a network of Local Partners and technologists, ahead of strategic capacity-building. During the final years of the ISC, new indicators were added to facilitate gathering and analyzing information under the internet freedom-focused objective. During FY2020, ISC made a strategic decision not to hold the Global Workshop and regional conferences in lieu of funding more initiatives that promoted ISC's sustainability, such as ToT trainings and in-kind grants.

Indicator Performance Tracking Table

Objective 1: Improve ICT security capacity of local partner organizations									
Ind	**Sub-IR**	**Indicators**	**Baseline 2017**		**FY18**	**FY19**	**FY20**	**FY21**	**LOP**
Output Indicators									
1	1.1	Number of People Trained	4,038	Target	500	500	300		4,678
				Actual	902	1201	3711	38	9,890
				Variance	402	701	3411		5212
2	1.2	"Number of organizations (civil society, social, independent media) assisted by program"	485	Target	50	50	25		560
				Actual	126	99	777		1,487
				Variance	76	49	752		927
3	1.3	Value (in USD) of in-kind grants donated to local partners	$109,185	Target	$25,000	$25,000	$25,000		$194,568
				Actual	$5,918	$12,942.32	$88,777.38	$91,864.00	308,687
				Variance	-$19,082.15	-$12,057.68	$63,777.38		$114,119
4	1.4	Number of regional workshops hosted	24	Target	8	8	3		41
				Actual	7	9	1		41
				Variance	-1	1	-2		0
5	1.5	Number of ToT candidates trained	48	Target	12	10	7		80
				Actual	93	111	96		348
				Variance	81	101	89		268
Outcome Indicators									
7	1.7	"Percentage increase in aggregate knowledge of information security principles and practices among local partners trained by the ISC"	57%	Target	50%	50%	50%		50%
				Actual	56%	52%	52%		53%
				Variance	6.0%	2.0%	2.0%		3%
8	1.8	Number of individuals subsequently trained by ToT candidates	2,053	Target	350	350	200		1,750
				Actual	1233	355	1499		5,140
				Variance	883	5	1299		3,390

Ind	Sub-IR	Indicators	Baseline 2017		FY18	FY19	FY20	FY21	LOP
Objective 2: Engage with specialized audiences and marginalized populations through outreach and partnership development									
Output Indicators									
9	2.1	Number of activities targeting specialized and/or marginalized populations	11	Target	10	10	5		45
				Actual	9	12	16		48
				Variance	-1	2	11		3
10	2.2	Percentage of people trained who are female	46%	Target	45%	45%	42%		46.5%
				Actual	48%	40%	51%		62%
				Variance	3%	-5%	9%		15%
12	2.4	Number of global workshops hosted	6	Target	1	1	1		9
				Actual	1	1	0		8
				Variance	0	0	-1		-1
Outcome Indicators									
13	2.5	Number of independent partnerships created	138	Target	35	35	17		220
				Actual	37	24	3		202
				Variance	2	-11	-14		-18
Objective 3: Foster the development of improved technology-based solutions to information security threats									
Output Indicators									
14	3.1	Number of small technology grants awarded	15	Target	8	3	0		23
				Actual	4	5	8		32
				Variance	-4	2	8		9
15	3.2	Number of tools tested and feedback provided to developers	86	Target	15	15	8		105
				Actual	19	13	28		146
				Variance	4	-2	20		41
16	3.3	Number of exchange visits between local partners and technology developers	5	Target	2	1	1		11
				Actual	3	1	0		9
				Variance	1	0	-1		-2

Objective 4: Enable civil society stakeholders to advocate on behalf of Internet governance and Internet Freedom issues and/or legislation									
Ind	Sub-IR	Indicators	Baseline 2017		FY18	FY19	FY20	FY21	LOP
Output Indicators									
17	4.1	Number of people trained on Internet governance and Internet freedom	50	Target	80	40	40		240
				Actual	60	0	20		130
				Variance	-20	-40	-20		-110
18	4.2	Number of advocacy campaigns developed and launched	0	Target	3	3	2		8
				Actual	4	6	10		20
				Variance	1	3	8		12
19	4.3	Number of small grants to advocacy organizations	4	Target	7	7	6		24
				Actual	3	6	10		23
				Variance	-4	-1	4		-1
20	4.4	"(F-indicator) Number of CSOs receiving Counterpart assistance engaged in advocacy interventions"	0	Target	4	4	2		13
				Actual	13	6	10		29
				Variance	9	2	8		16
21	4.5	"Number of individual research documents produced on relevant Internet freedom issues"	0	Target	3	3	0		8
				Actual	9	2	16		27
				Variance	6	-1	16		19
22	4.6	"Number of events related to internet governance or internet freedom with significant participation by Counterpart and partners"	2	Target	3	3	2		8
				Actual	16	7	37		62
				Variance	13	4	35		54

Part Four: Implementation Successes and Challenges

Of the USD 24 million allocated to the ISC, ~70% was spent on cybersecurity support for CSOs and independent media organizations, ~15% was spent on eight annual Global Workshops, ~10% was spent on support for policy advocacy, and ~5% was spent on technology development.

ISC's Digital Security Specialists eliminated tens of thousands of cyberinsecurities for developing-world activists and journalists, thus reducing their attack surface and dramatically reducing their adversaries' ability to impede their work. In this way, the ISC supported the efforts of CSOs and independent media organizations to keep civic spaces open in challenging environments.

During the ISC, the relative importance of the cyberinsecurities eliminated by Digital Security Specialists changed, resulting in new challenges in what they worked on, how, and with what complications. For example, attackers regularly discover and leverage bugs in common software to compromise users of that software, prompting software makers to patch those bugs to keep end users safe. Users of pirate software, however, do not get the patches, resulting in their vulnerability to an ever-increasing number of unpatched bugs. The importance of remediating the vulnerabilities resulting from running unpatched software, particularly pirated Microsoft Windows and Microsoft Office, Adobe Acrobat Reader, and out-of-date Chrome and Firefox browsers, escalated over time. Fixing this issue in the case of Microsoft software is significant as each Windows or Office license costs ~USD 200. No activist or journalist is going to choose to spend USD 400 if they can acquire and run pirate software for free. In reality, buying all this software at market prices would have eaten up a large portion of the ISC's budget, so Counterpart and others doing this work lobbied Microsoft to address the issue. Shortly after the ISC's inauguration, Microsoft agreed to provide its software licenses to NGOs at a dramatically reduced rate through TechSoup. As a result, the ISC quickly became one of TechSoup's biggest global customers, deploying thousands of licenses to Local Partners' staff devices.

When ISC began its work, passwords were the ultimate tool of online account security. As attackers began hacking the user databases of online services – such as LinkedIn, Yahoo!, and Adobe – and successfully reusing stolen passwords on other services (a practice known as credential stuffing), the importance of unique passwords increased. Because most users cannot remember dozens of unique passwords, the password manager was invented, and ISC's Digital Security Specialists began helping Local Partners learn how to obtain and use password managers such as LastPass and 1Password. Additionally, though the introduction of 2FA added an important new cybersecurity defense mechanism, few people heard about or understood it on their own. ISC's Digital Security Specialists were instrumental in helping Local Partners deploy 2FA to defend important online accounts on platforms like Google, Apple, and Facebook. After cloud computing arrived, many services migrated across and the importance of defending online accounts with good passwords and 2FA increased in relative importance.

Neutralizing Cybersecurity Threats

The ISC's structure as a USAID Washington-funded grant with no mandated countries, and thus no inherent permission to work in certain regions, added a complicating element to the ISC's implementation. Initially, responsibility for selecting countries in which to work required obtaining permission from the relevant USAID mission, which ultimately tracked back to USAID itself, effectively cutting the ISC out of the loop. Over time, however, Counterpart became more proactive in proposing new ISC countries, enabling the ISC Chief of Party to adapt to working with the ISC Agreement Officer Representative to identify new countries, initiate mission clearance requests, and shepherd requests through the approval process.

In some cases, no response from a USAID mission was received; in other cases, missions reacted warily or even negatively. Yet, once missions understood ISC's goals and *modus operandi*, and that nothing – especially money – was being asked of them, they began to get

comfortable the ISC team and its work, while not easily understood, would be widely beneficial. At the same time, the ISC learned to quickly accept "no" for an answer when requesting Mission approval, so as to move on and identify countries that welcomed the services on offer. As a result, the country count increased significantly, particularly during the last year of the ISC, leaving Counterpart to conclude it would have made sense to take a more proactive approach from the beginning.

The ISC was originally designed to pick up where cybersecurity workshops for civil society organizations in the 2000s had left off, extending beyond talking to actually teaching people what they needed to do to stay digitally safe while helping them do it. The ISC's model proved very successful at accomplishing its primary goal of neutralizing cybersecurity threats for those it sought to help, removing hundreds of thousands of cyberinsecurities for tens of thousands of activists, journalists, NGOs, and independent media organizations and installing strong, lasting defense mechanisms. However, if an organization the ISC supported fails to apply the same cybersecurity attention to new employees, then cybersecurity defenses will begin to fail. Although part of an ISC Digital Security Specialist's task included encouraging Local Partners to adopt and enforce simple IT policies and implement baseline cybersecurity defenses, institutionalizing cybersecurity in a long-term way is potentially challenging.

The ISC made progress eliminating the problem of cybersecurity by embedding into daily life the necessary defenses to such a degree that failure simply did not happen. But the minute the ISC finished work in one country and moved on to another, the previous country's civil society immunity against cyberattacks began to degrade. CSOs and independent media organizations remained vulnerable to decreased vigilance and bad habits, as well as the need to replace equipment with new, and often less secure, equipment. With limited resources, these groups would also be unlikely to pay IT specialists to maintain their defenses. If preserving civil society actors' cybersecurity is of paramount importance, then the donor community will need to continue supporting the initiatives undertaken by the ISC as it is unrealistic to assume civil society has the capacity to go it alone.

Although the ISC positively impacted a specific set of problems and solutions, it would have benefitted from prioritizing the most important cybersecurity issues. The community supporting cybersecurity in restricted civic space would have been better off monitoring what problems actually compromised those the ISC was defending and focus its limited resources on resolving only those problems. For example, far too many resources are still invested in discussions about which instant-messenger system, software, or network is better, ignoring the more important issue that CSOs and journalists must stop using POTS / PSTN (Plain Old Telephone Service / Public Switched Telephone Network) because it is not at all secure; any and all instant-messenger applications or networks are far more secure.

Even more importantly, beneficiaries should be urged to cease using pirate software, which cannot be patched and is highly vulnerable to cybersecurity threats, simply because it costs money to replace or because it is open-source – open-source products have their advantages, but embedded cybersecurity is not one of them.

Identifying Trusted Local Experts

The ISC found that it essential to identify people in-country who were local experts, and who were trusted within the civil society community. Not only was this more effective in terms of logistics and cost, but proved to be a key element in the success of planned interventions – without trust, there was no openness to engaging with Digital Security Specialists.

Managing a Global Program

To ensure sound leadership and successful implementation, it is important to have managers who are not just technical experts, but possess strong interpersonal skills, cultural sensitivity, and a willingness to employ a diverse range of methodologies to support effective communication and decision-making.

From its inception, the ISC was designed to respond to USAID requests that attention be paid to specific countries. Securing buy-in from USAID Missions, however, was delegated to the USAID Agreement Officer Representative, inadvertently insulating Counterpart from the process. The result was the ISC increased its country coverage slowly as suggestions for expansion were received from USAID. A key factor in the ISC's success was buy-in at the country level, facilitated in places where Mission staff were knowledgeable about the importance of digital security and internet policy for protecting civil society spaces and activism. Where that understanding was lacking, Mission staff often failed to recognize the value or importance of the services offered by the ISC.

As the ISC progressed, so did the pace of geographic expansion. ISC began more assertive in identifying potential new countries, and better at working with the Agreement Officer Representative to request

clearance from USAID Missions. Ultimately, the ISC was able to expand its reach from ~ 20 countries to 36 countries in the final year and a half of the Project.

Flexible and Compliant Grant-Making

In early years of the ISC, grant-making consumed a significant amount of personnel time, with the level of effort greater than the cost of the hardware being procured. As ISC evolved, Counterpart reassessed grant mechanisms and grant-making processes, and invested in hiring a Senior Grants Manager who improved and simplified procurement and Local Partner subawards, especially for IFPA. A good grants manager can proactively design subaward terms that support a partner's strategy and milestones. By articulating results and milestones, and tying those to payments, Counterpart was able to streamline ISC grants and save significant time and cost.

Support cybersecurity, however, proved a rather broad mandate. Instead, the ISC chose to solicit grant proposals to solve actual cybersecurity problems faced by ISC's Local Partners. The resulting grants supported the technical testing of existing tools, linguistic translations of existing software interfaces, documentations, and training materials, the creation of product documentation and training materials, and the customization / improvement of existing tools. In short, the focus of ISC's funding was on improving existing tools rather than developing new ones. ISC allocated 26 technology support grants.

Sustainability and Journey to Self-Reliance

The ISC experience led Counterpart to conclude that cybersecurity is not something easily mainstreamed. To use an analogy, we could try to teach USAID program officers and local NGOs how a car engine works so they can conduct their own repairs, but this is not realistic because not everyone is going to become a mechanic. Car owners generally outsource maintenance and repair work to mechanics, either proactively by paying attention to warnings and indicators of health, or by waiting until something breaks down. ISC's approach was to teach people to understand enough about digital hygiene to know when they needed to ask for help from a Digital Security Specialist. Though the ISC was designed by USAID to fix the problem, it does not meet the rubric for promoting sustainable, self-reliance. That said, the ISC was tremendously successful in making Local Partners safe online. Looking ahead, as Local Partners continue to work in dangerous environments, ISC-like work needs to continue to be provided by external experts.

To use another analogy, the ISC was akin to socialized cybercare as most developing-country CSOs and independent media organizations had neither the resources to hire cybersecurity experts nor the time to dedicate to securing their networks – they are often too busy getting colleagues out of prison or writing lengthy and onerous grant proposals. Additionally, most developing-country markets do not have IT personnel *au courant* with the cybersecurity mitigations that the civil society community needs. As a result, the ISC was compelled to hire local Digital Security Specialists to oversee cybersecurity care for the CSO community, and support dozens of Local Partners made up of hundreds of activists and journalists). USAID is to be commended for having imagined this model in 2011, and Counterpart is honored to have been able to implement it.

Early on, ISC's managers hatched a plan to encourage in-country Digital Security Specialists to institutionalize themselves as local cybersecurity-providing NGOs. Though most were unenthusiastic about this concept, in two countries (Zimbabwe and Ukraine) the idea was operationalized by creating the Digital Society of Zimbabwe and the Digital Security Lab (DSL) in Ukraine. As of writing this report, the DSL is successfully operational, busy, and funded by many donors who support internet freedom work. Sadly, DSZ has gone quiet with little interest from donors or civil society actors to finance their work. ISC concluded that this localization model can work if it is driven locally by the right person or entity, and if there is significant donor interest in that specific country, which could spill over to support cybersecurity work.

Since the ISC's inception was motivated by the understanding that complicated cybersecurity solutions either did not work or would not be adopted or maintained by those the ISC was created to help, Counterpart sought out cybersecurity solutions that could be undertaken as a one-off, akin to *vaccination*. Over time, a basic vaccination panel evolved, and by the end of the ISC consisted of ~15 issues, each with its own "set and forget" solution, which Counterpart's in-house DSS Helper application audited and tracked.

As with real-life vaccinations, ISC's cybersecurity fixes needed boosters in order to remain effective. At a minimum, this involved periodically examining existing fixes to ensure they remained encrypted. Some boosters – provided the original fixes were done correctly – should be updated automatically. For example, *"has the operating system (Windows, macOS), productivity suite (Office), or browser (Chrome, Safari) applied the updates that were most recently released?"* Some boosters might become necessary because the end user has acquired a new risk – e.g., if a journalist decided to start communicating with in-

government whistleblowers, they would need to use a secure messenger, as well as a secure metadata-less messenger to eliminate the possibility of a bad actor learning who was communicating with whom (such as Ricochet or Briar). Some boosters offered new, more effective solutions to old problems, such as upgrades to 2FA to protect online accounts by adding applications like Taya to the mix, which offered measurable benefits for high-risk users. Some boosters anticipated new risks, such as an inevitable migration from 4G to 5G, which will no doubt provide new technical capabilities to beneficiaries, but will also further enable their adversaries.

Using ToTs to train Local Implementers and connecting Local Partners with one another in a given country was an attempt to institutionalize a regular, scheduled boosters. As was the embedding of a Digital Security Specialist into an NGO providing cybersecurity services (e.g., Zimbabwe's DSZ and Ukraine's DSL). A third, similar, attempt involved allocating subawards to local NGOs that were willing and able to begin fulfilling the ISC's cybersecurity-providing functionality to the community (e.g., Venezuela's REDES, Belarus' Barys Zvozskau).

Stories of Inclusion

The ISC provided focused support to specialized and marginalized communities who faced specific or heightened digital security threats due to their already marginalized position within society. Women, youth, indigenous populations, religious minorities, and LGBTQ organizations were trained and mentored within each of ISC's countries of implementation. Specialized communities included human rights defending lawyers, environmentalists, independent media organizations, and other groups who had the ability to promote or protect the digital security work and practices of Local Partners.

Women's Empowerment

In FY2016, the ISC improved its country assessment reports by enhancing its research methodology and diversifying content sources so each new or updated report was peer reviewed by a Gender and Social Inclusion specialist, whose input would add critical perspective to the threats faced by marginalized communities in particular.

In FY2019, the ISC's Southern and East African Digital Security Specialist attended an event for regional responders hosted by the *Open Society Initiative for Southern Africa*. The goal was to map current digital security support efforts in the region and identify gaps. The main gap identified was the lack of investment in female ToT, which contributed negatively to a shrinking network of digital safety experts. Conference goers also identified the need for a regional strategy to maximize existing capacities and synergies to increase digital safety support for vulnerable environmental rights groups in South Africa.

In Nicaragua, the ISC's Digital Security Specialist developed a feminist approach to digital security, which she has been sharing with women-focused NGOs. The approach was developed by female activists and journalists who faced online attacks, who are now using their testimonies to empower other women to take digital security into their own hands. Certain online attacks predominantly target women, such as revenge porn, and this feminist methodology utilizes material from survivors to facilitate a safe space for discussion and reflection on technology's role in gender-based violence. During Nicaragua's 2018 upheaval, gender-based violence online was utilized specifically against women protestors to deter their activism. Today those same activists are leading workshops to address topics like Netiquette (online ethics), image care (e.g., how to take action if photos are distributed without authorization), preventative measures and securing social media accounts, and safe sexting.

Support for LGBTQ Persons

LGBTQ activists face unique and growing threats when using online and mobile applications for networking and advocacy. To help highlight these concerns, the ISC hosted a panel discussion in New York City in September of 2015 that brought together developers whose applications supported LGBTQ communities (e.g., Grindr), and activists advocating for LGBTQ rights (e.g., Internews, EngageMedia, OutRight Action International, and Access). Discussions focused on how new technologies and mobile applications can empower activists, but also can be used to exploit and endanger individuals or their networks. Online social media and dating applications, such as Grindr, Scruff, and Facebook, are popular with LGBTQ communities as they allow individuals to interact and form communities. This type of interaction not only helps those who previously felt isolated, but also allows groups and individuals to organize and advance LGBTQ activism.

As useful as these tools are, however, they may also expose users to greater risk. Adversaries can exploit these sorts of technologies through sophisticated surveillance and impersonation methods that enable access to usernames, passwords, and other personal information. While panelists agreed that the benefits of these tools could not be denied, they emphasized that users should understand the risks before using them. The threat of computer and mobile phone confiscation is also a serious threat to LGBTQ activists, as law enforcement agencies in many countries use this approach to gain access to an individual's contacts in order to expand the targeting of LGBTQ individuals. The panel also discussed specific threats associated with LGBTQ dating websites. Grindr, the most popular dating application among gay men, recently launched Grindr for Equality, a social platform that provides geo-positioning data to inform users of relevant events in their local LGBTQ community. However, because of the risks associated with geo-positioning information being intercepted in some countries, Grindr has disabled the feature in certain regions.

In late October 2016, ISC staff participated in a discussion panel highlighting threats to the transgender community in Africa at the Southern Africa Transgender Forum in Johannesburg, South Africa. The panel discussed digital security topics to help the 60-person audience understand threats they could face using social media and dating applications. The ISC not only provided its expertise, but also used the opportunity to engage in outreach activities, which resulted in one new Local Partner from the Zimbabwe transgender community.

Throughout the summer and fall of 2019, many Balkan countries hosted their first-ever pride parades (e.g., Bosnia and Herzegovina, and North Macedonia), marking a positive shift in the relationship between the LGBTQ community and broader society. The ISC's Balkan Digital Security Specialist met with the main event organizers in both countries and learned that, to save costs, the Bosnian organizers were using shared hosting for their website. The Digital Security Specialist explained the risks of doing so, and made an in-kind grant for secure webhosting through a technology partner at Greenhost, as well as DDoS protection through technology partner eQualitie's Deflect tool (deflect.ca). As a result, no website attacks were reported.

In March 2020, the ISC's Digital Security Specialist in Tajikistan was instrumental in assisting an LGBTQ activist whose life was in danger after nightclub footage surfaced online showing the individual being intimate with someone of the same sex. Akhbor.com, as well as a number of anti-LGBTQ Facebook groups, reposted the video. The Digital Security Specialist moved quickly to contact the administrators of the website and social media groups to have the video removed, explaining the breech of privacy, as well as the illegality of inciting violence. She later held a session for the activist's entire organization on how to secure photo archives and safely send intimate pictures through encrypted messaging. There was also a discussion of Netiquette and the effect of cyberbullying on vulnerable groups.

Support to Indigenous Communities

In 2019, the ISC's Tanzanian Digital Security Specialist began supporting six indigenous groups in the Moshi, Kilimanjaro region, including the Pastoralists Indigenous Non-Governmental Organization's Forum (PINGOs), Media Advocacy for Indigenous Peoples Community, Community Research and Development Service, the Tanzania Natural Resources Forums, the Tengeru Institute of Community Development, and the Pastoral Women's Council. Activists from rural areas faced acute threats, as hardware, software, and overall resources were older and poorer than in urban areas. The ISC provided each Local Partner with official Office licenses, and set devices to automatically patch. As another cost-saving measure, the Tanzanian Digital Security Specialist recommended a set of free, open-source tools for ensuring day-to-day security, including cloud backups, virus defenders, password managers, and message encrypting services. Workshop participants were eager to share these new tools with staff members not in attendance, but worried about the poor internet connection at their home offices – yet another obstacle for those in the countryside. USBs were subsequently pre-downloaded with certain programs to counter this issue.

In October 2020, the ISC's Digital Security Specialist in Brazil worked closely with Local Partner Instituto Internacional de Educação do Brasi to develop a digital security curriculum based on experiences relevant to daily lives of indigenous persons. Challenges related to low internet access, language barriers (Portuguese is not the main language for most Amazonian communities), and the fact that few indigenous persons had any prior education in digital security led the Digital Security Specialist and IEB to rely on the input of other groups with experience mobilizing this population online. Media India, a media platform led by indigenous persons, was invited to make an opening speech during the training webinar to contextualize the importance of being safe online within their lived experiences by focusing mostly on Facebook and WhatsApp. Another group, Intervozes, presented the results of their study on issues related to low internet penetration by indigenous communities, and offered recommendations for expanding access. These collaborations between media and research groups focused on the Amazon proved successful providing visibility to marginalized groups in Brazil.

Part Five: Operating Effectively and Efficiently

The ISC encountered management challenges during implementation, including staff turnover, gaps in knowledge and institutional memory retention, distribution of personnel time and resources, and transitions in leadership. These obstacles were sometimes compounded by the decentralized and global nature of the ISC. By testing different implementation strategies, ISC staff were able to iterate until a working management approach was formulated, and eventually adapt as ISC expanded. This flexibility was crucial in implementing different phases of the ISC, as evidenced by ISC's overall effectiveness and achievements during its lifespan.

Ensuring Cost Effectiveness

The ISC–being one of two global projects implemented by Counterpart–was the first to establish a bespoke operational model for a multi-country project that lacked a robust physical presence, but had no specific ISC central command. Considering the coverage of the ISC, the number of actors involved, and the issues related to secrecy and security, Counterpart quickly realized that operational and administrative management must be centralized at the HQ level.

Organized regionally, an HQ Program Officer was assigned to each region to manage the administrative implementation of in-country activities, which included procurement, travel, HR, security, and grant-making. As a result, the ISC was directly served by HQ support units, including Human Resources, Security, Grants and Compliance, and Finance, all of which minimized time, cost and the need for additional services. The direct oversight by Counterpart's HQ staff also facilitated rigorous administrative management in compliance with Counterpart's internal policies and regulations, including its Procurement Policies, Grants Manual, Financial Management Policy, Travel Policy, and others.

Key elements of the centralized operational model included:

- In-country Digital Security Specialists were hired on a consultancy basis, which proved flexible for Counterpart and the Specialists, and saved significant costs for the ISC . Digital Security Specialists were paid for actual tasks performed under the supervision of Regional Managers, and only after approval of all deliverables.
- Regional Managers were hired locally as employees to operate from their country of residence, which resulted in a significant cost savings related to allowances and other employee benefits.
- All travel was organized, procured, and managed by HQ officers.
- All procurements for hardware allocated via in-kind grants were administered locally by Digital Security Specialists, which saved transaction and shipping costs.
- All procurements of software and other online products were administered by HQ, which minimized transaction costs and expedited the delivery times.
- Centralizing grant-making at HQ allowed it to be combined with in-kind donations, which resulted in significant cost savings and benefits.
- By being located at HQ, the ISC was able to avoid paying for field office rent and similar costs related to operations.

This centralized model of operations proved to be both efficient and effective – stretching a budget of USD 24 million to reach out and provide continuous support to nearly 10,000 beneficiaries in 36 countries for almost a decade – which made the cost per beneficiary just less than USD 2,500 (inclusive of in-kind donations and the costs of materials).

Adaptations in Grant-Making

In its willingness to adapt to a diverse implementation universe, the ISC was able to issue cost-reimbursable, simplified, fixed amount, and in-kind donation agreements. These subawards were issued using both competitive and non-competitive processes to support ISC objectives 1, 3, and 4.

Objective 1: Improve the ICT Security Capacity of Local Partner Organizations

Issue In-Kind Donations to Local Partners to Reach a Necessary Level of Cybersecurity Defense

The assessments conducted by the Digital Security Specialists for each Local Partner included recommendations for software and hardware solutions to safeguard IT infrastructure and enable staff to implement best practices in digital security. The Regional Managers reviewed and validated assessments and approved, subsequent to CoP review, donation requests before in-kind grants were issued.

To ensure donations realized value for money, the ISC facilitated the registration of all eligible Local Partners with TechSoup, gaining access to discounted and or free licensed Microsoft, Adobe, Bitdefender, and other software. All hardware procurements were executed in accordance with Counterpart's organizational procurement policy.

Over the course of the program, the ISC issued 219 in-kind donation agreements to support Local Partners. The most common vulnerabilities and remedies cited were:

Vulnerability Assessed	Threat Produced by Vulnerability	Suggested Remedy
Use of unlicensed, outdated, or otherwise unsupported software	Lack of access to automatic security updates provided to licensed versions of software	Donation of licensed software; donation of hardware components or new hardware to ensure that Local Partner can utilize modern software
Lack of virus and/or malware protection	Elevated risk of data loss through virus or loss of sensitive information through malware	Donation of active anti-virus & malware software
Lack of data protection and backup procedures	Elevated risk of data loss through accidental or criminal means	Donation of hardware to facilitate a data backup regime

Adaptations

The global, decentralized nature of this activity limited its scope and meant that each Digital Security Specialist had their own network of Local Partners to train and support, which in turn limited the amount of time available for each. As a result, in-kind grants were not incorporated into longer-term capacity building plans so that ISC could monitor the use and effectiveness of specific donations on digital security capacity. The grant agreements did not stipulate the use or objectives for improvements, meaning from a grant-making perspective the activity was completed once donations were received, installed, and verified. The lesson learned was that if projects want to measure the effectiveness or capacity gains of in-kind grants for software and hardware, the grant agreements should include follow-up between the project and partner.

Issue Subawards to a Local Implementer to Take Over the Cybersecurity Defense

The ISC issued 23 subawards to Local Implementers who approached the ISC with unsolicited proposals to conduct their own digital security activities. These proposals would first be reviewed by the relevant ISC Regional Manager and Digital Security Specialist, each of whom would evaluate them on technical merit and organizational capacity. The ISC CoP would then perform a secondary review and, once a request was approved, the ISC Grants and Management team would manage the process.

The process used to issue Local Implementer grants began with a pre-award assessment to evaluate the organizational and financial capacity of the subawardees, followed by a review of the nature of proposed activities, and an analysis of the existing operational and political risks facing those activities. Together, these activities would inform whether to use reimbursable, simplified, or fixed agreements, as well as the creation of a risk management and monitoring plan for the subawardees. In almost all cases, ISC Local Implementers lacked the capacity to implement reimbursable grants at acceptable levels of risk, necessitating the use of fixed amount awards.

Grant negotiations would then occur, wherein the ISC would verify proposed activity costs did not exceed actual costs above a specific increment, and agree a milestone plan – including payment amounts and requirements for unlocking payments, as well as a calendar for deliverables and deadlines. Once agreed, USAID Agreement Officer Representative approval would be requested, while the proposed agreement underwent initial and clearance reviews at Counterpart HQ.

Adaptations

As this activity could only be implemented when Local Implementers demonstrated the capacity and willingness to conduct their own digital security activities, they did not undergo a competitive process. Furthermore, there was no written criteria or benchmarks through which the Regional Manager could quantify what constituted requisite capabilities. It is not coincidental that Local Implementers were less responsive and engagedt in the grant-making process, both in terms of pre-award negotiation and compliance requirements during implementation,. Because of the urgency of the assistance needed, Counterpart did use quick, noncompetitive grants judiciously in order to respond to Local Partners. Under all other circumstances, Counterpart's preference would be to run a proper competitive process for grants.

Issue Microgrants to ToT Trainees to Support and Expand Cybersecurity Support and Reach

The ISC issued 15 ToT microgrants to individuals or organizations who had been specifically identified by ISC Digital Security Specialists and Regional Managers. Given these grants were made to individuals to conduct a set number of digital security trainings, they were issued as fixed amount grants at the highest level of risk monitoring. In all other respects, the grant-making process was identical to the grant processes used for Local Implementers.

Objective 3: Foster Development of Improved Technology-Based Solutions to Information Security Threats

The ISC issued 23 subawards in support of this objective through publicly advertised Requests for Applications (RFAs) were published for grant cycles in 2013, 2016, 2018, and 2019. Applications were evaluated by a selection committee of digital security experts from the ISC, as well as from Counterpart's network. Once the winning applicants were selected – based upon criteria established in the RFAs –ISC entered into negotiations to ensure that fixed amount awards did not compensate subawardees above actual costs. Subawardees were also subject to Counterpart's organizational review and screening process. All subawardees under this objective were issued fixed amount awards, and due to the small and inexperienced nature of most of the selected developers, were assigned the highest level of risk monitoring.

Adaptations

Fixed amount awards were not the ideal choice for software development. In several cases, unexpected IT development delays necessitated modifications to milestone calendars and periods of performance. While most of the technology development subawardees lacked the internal systems and liquidity necessary to implement reimbursable grants in compliance with USAID and Counterpart requirements, the result of relying on fixed amount awards to support potentially unpredictable software development was underpayment when subawards were extended at no cost.

Objective 4: Enable Civil Society Stakeholders to Advocate on Behalf of Internet Governance Issues and Legislation

The ISC issued 24 subawards in support of this objective through publicly advertised RFAs for grant rounds in 2017, 2018, and 2019. In 2020, the ISC Project utilized an APS mechanism with the intention of supporting organizations on a rolling basis throughout the year. Under both RFA and APS mechanisms, applications were reviewed by selection committees comprised of ISC technical experts, and followed up by the same grant negotiations and compliance review processes described above. Fixed amount awards were the primary grant mechanism utilized, reflecting both the nascent capacities of subawardees and the predictability of advocacy-related activity costs.

Adaptations

As initial grant cycles yielded a modest number of applicants, the ISC did not anticipate the breadth of interest in advocacy grants for 2020, and by the first deadline of the APS, the ISC received more applications than it could realistically support.

The ISC Project

2345 Crystal Drive
Suite 301
Arlington, VA 22202
USA

+1-571-447-5700
communications@counterpart.org
counterpart.org