UC BERKELEY
CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Digital Safety Technical Assistance at Scale

SEAN BROOKS

CLTC WHITE PAPER SERIES

Digital Safety Technical Assistance at Scale

SEAN BROOKS

CITIZEN CLINIC

JUNE 2020

UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

Acknowledgments

Citizen Clinic and the Center for Long-Term Cybersecurity would like to thank the partners and clients of the Citizen Clinic program, without whose trust and dedication none of our work in this space would be possible.

Special thanks to Ann Cleaveland, Steve Weber, Steve Trush, and Chuck Kapelke of CLTC for their advice, feedback, support, and contributions to this paper.

CLTC would like to thank Microsoft for a gift that supported this research.

Contents

Executive Summary

Around the world, civil society organizations — including human rights organizations, Indigenous groups, journalists, and many others — are targeted online by powerful, well-resourced adversaries, including governments. Yet most civil society organizations lack the funding and expertise needed to defend themselves against cyberattacks, disinformation campaigns, digital surveillance, and other threats. This paper explores the opportunities and challenges of expanding digital safety technical assistance to civil society at a scale and pace that match the sector's needs.

Drawing in part upon our experience in leading the University of California, Berkeley's Citizen Clinic, through which teams of students provide digital safety services to politically targeted civil society organizations, the paper offers practical guidance on what will be needed to deliver cybersecurity assistance on a larger scale. Focusing on the desired outcomes of such an effort, we provide examples of diverse technical assistance projects, as well as tactics from sectors outside the cybersecurity space. At the conclusion, we evaluate three potential mechanisms for scaling technical assistance for civil society — volunteer networks, cybersecurity clinics, and community hubs — and analyze their strengths and limitations.

Among the key findings outlined in this report:

- The first step in improving the digital safety posture of civil society often does not mean "hardening" organizational systems, but rather helping overcome a perceived lack of agency. Improved security assistance needs to move civil society organizations to a point where they can withstand a basic attack, in order to generate the necessary confidence to take greater ownership of managing digital risk.
- In order to be effective, efforts to scale cybersecurity technical assistance for civil society must accomplish three interdependent outcomes: quality of service, increased organizational capacity, and a stronger technical assistance ecosystem.
- Finding new pathways for onboarding less-experienced professionals into the space is critical to providing more helping hands.
- Volunteer networks of experts can greatly expand the scale of assistance, and may have untapped potential for improving the state of the ecosystem. They have a track record of responsiveness to emerging needs, and can leverage the desire of many security professionals to share their skills beyond their day jobs. However, volunteer efforts require oversight mechanisms not yet in existence, and must be closely monitored to ensure their

quality and long-term impact, as expert volunteers may not have experience with the nuances of supporting civil society.

- University-based clinics address many of the challenges of scale in a cost-effective way. Clinics can specialize and build deep ties with communities, experiment with new methodologies in a rigorous manner, and create a pipeline for skilled assistance providers. However, any single clinic is unlikely to deliver significant scale to technical assistance.
- Community hubs — organizations designed to provide digital safety services to specific communities in need — are an understudied model for providing technical assistance to civil society. Such hubs can move swiftly to provide direct technical assistance with relatively few startup costs, and can manage both capacity-building projects and emergency response efforts. However, these hubs are sometimes expected to be "everything to everyone" in their communities, and the level of support expected of them can be difficult to maintain.
- Technology platforms and providers can provide assistance, and governments can compel certain security, safety, and privacy-enhancing design decisions. But policy and products designed to serve the social good must be responsive to the requirements articulated by an active, connected, and high-functioning set of digital safety experts who are deeply engaged with civil society on a regular basis.

The technical assistance models examined in this report all provide different potential benefits, but all contribute differently to scaling digital security services for civil society organizations. The future will require innovation and experimentation to develop models and communicate about the risks to policymakers, technology firms, funders, researchers, and senior leaders in civil society. Activating already existing expertise and helping organizations utilize existing channels for support are important elements, but we must also expand the number of professionals in the space. A more nuanced perspective on the digital safety challenges facing civil society organizations is essential not only for providing a high quality of service, but also for designing appropriate technical products and policies.

"Happy families are all alike; every unhappy family is unhappy in its own way."
—Leo Tolstoy, *Anna Karenina*

Introduction

In 2018, following the Center for Long-Term Cybersecurity's research into gaps in the cybersecurity technical assistance ecosystem, we developed the Citizen Clinic program to provide contextually informed digital safety services to politically targeted organizations. Structured as a course within UC Berkeley's School of Information, the program follows the examples set by clinical education systems in law and medicine. It provides students with an opportunity to practice cybersecurity in a real context, and offers services that would otherwise be unaffordable to many civil society organizations (CSOs). To date, Citizen Clinic has educated over 60 students from nine different academic programs, including computer science, law, public policy, journalism, and information science. We have supported 10 organizations across four continents and many diverse communities, including organizations that advocate for reproductive, Indigenous, and gender rights, as well as organizations that investigate international abuses of human rights law and development.

We have refined our educational pedagogy, and structured the clinic both as a workforce pipeline for public-interest technologists and as a vehicle for improving the practice of technical assistance. But we still have not scratched the surface of the challenge. Civil society continues to move online (even more so, given the COVID-19 pandemic), taking advantage of an internet ecosystem that offers many opportunities for decentralized collaboration, community building, and intersectional activism. And yet, as explored in our previous report, the sophistication of online adversaries continues to grow.[1] While we believe the contribution of this new model for technical assistance is significant (similar clinical programs have already emerged at other universities), the question remains: *how can we expand the scale of technical assistance to match the demand from civil society organizations around the world?*

Given the growing threats, we cannot accept the slow rate of change we've seen in more advanced private companies and public institutions. This issue is reminiscent of Christensen's

1 Brooks, Sean. 2018. *Defending Politically Vulnerable Organizations Online*. Berkeley, CA: Center for Long-Term Cybersecurity, https://cltc.berkeley.edu/defendingpvos/

Innovator's Dilemma;[2] iterative change in technical assistance models will only provide incremental advantages to civil society organizations' security. **More substantial market shifts are necessary to address the needs for civil society security at scale, and at pace, to match the need.**

While the challenges of scale are perennial in public interest work, addressing this issue specifically through the lens of cybersecurity technical assistance leads to additional questions that must be answered. *What* exactly needs to scale — individuals' skills, organizational capacity, or the number of technical assistance practitioners? What *outcomes* are we pursuing — better operational integrity, improved global free expression, or the safety of civil society professionals? And finally, what *mechanisms* might supply the right types of outcomes for civil society? By evaluating the qualities we are trying to scale, we can ascertain what models for providing assistance lend themselves to those organizational or societal attributes.

This paper explores the desirable outcomes of providing cybersecurity assistance at scale to civil society. We break these into three sets of potential outcomes at different levels of abstraction: for effective service provision, for improving the capacity of CSOs to manage digital safety risks, and for improving the broader state of the assistance ecosystem. We provide examples of how these outcomes are being pursued through diverse technical assistance projects, and offer examples of different tactics from sectors outside the cybersecurity space. Throughout, we include anecdotes from the first two years of practice within Citizen Clinic to share some of our learned experience. At the end of the paper, we evaluate three potential mechanisms for scaling technical assistance for civil society — volunteer networks, the clinical model, and community hubs — and analyze their potential and limitations, based on the outcomes defined.

But what changes are the "right" changes for civil society and their supporters in the digital safety space? In the next section, we define seven potential outcomes for the quality of technical assistance, organizations' internal capabilities, and the broader ecosystem of providers, in order to establish measures for evaluating models' ability to provide assistance at scale.[3]

2 Christensen, Clayton M. 1997. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston, MA: Harvard Business School Press.

3 The outcomes were designed based on positive feedback we have received in Clinic work, research we have conducted into gaps in the technical assistance ecosystem, and needs we have identified as we have tried to provide high-quality services to our partners. This list is not designed to be exhaustive, but rather a summation of the high-level improvements to the ecosystem, organizations, and technical assistance quality we believe would most meaningfully improve the state of civil society's digital safety.

KNOWN CHALLENGES TO SCALE

The rapid pace of change in technology is often cited[4] as a major pressure on defenders in the cybersecurity arms race. Yet our work has reinforced what many experts told us in 2018: low-cost, low-sophistication attacks are a leading challenge to civil society organizations. There is no reason why a threat actor — even one with vast resources, like a government or multinational corporation — should spend hundreds of thousands of dollars on zero-day attacks when a simple phishing email will do. However, just because technical solutions are available does not mean they are easy to implement. And while many of the needs of civil society organizations are similar, the order in which improvements can be made, and the technology choices and cultural changes that need to complement those deployments, require careful attention to the specific context of each organization. Citizen Clinic's contextually-informed risk assessments are a critical component of our work, but present a serious challenge to scale: if one size does not fit all, how do we provide customized cybersecurity support for a mass audience?

A Cybersecurity Market Failure

Nonprofits spend on average about 5.7% of their total budgets on IT, ranging from 1.5% in large organizations to 13.2% in small organizations.[5] Private-sector firms spend about 3.3% of their total *revenues* on IT, ranging between 1.5% in the construction industry to 7.2% in banking.[6] These numbers may look comparable — perhaps even giving non-profits the edge — but for organizations whose entire budget is built on fundraising or subsistence-level business models, the difference between *total budget* and *revenue* is profound.

IT spending *per user* tells another story: private-sector firms spent an average of $8,183 per user in 2018,[7] while nonprofits spent just $3,195 per user. That's a dramatic difference, and even in a best-case scenario, only 5–7% of that budget is earmarked for cybersecurity in the private

4 Rahman, Zara, et al. 2018. *The Ties That Bind: Organisational Security for Civil Society.* The Engine Room: https://www.theengineroom.org/wp-content/uploads/2018/03/Ties-that-Bind-Full-Report.pdf

5 Hulshof-Schmidt, Robert. 2017. "The 10th Annual Nonprofit Technology Staffing and Investments Report." The Nonprofit Technology Enterprise Network: https://www.nten.org/wp-content/uploads/2017/05/Staffing_Report2016_v12.pdf

6 Deloitte Insights. 2018. "IT Spending: From Value Preservation to Value Creation." *The Wall Street Journal: CIO Insights:* https://deloitte.wsj.com/cio/2018/03/12/it-spending-from-value-preservation-to-value-creation/

7 IT Spending and Staffing Benchmarks 2019/2020", 2020. *Computer Economics: https://www.computereconomics.com/page.cfm?name=it-spending-and-staffing-study*

sector.[8] That means per-user security spending in an average non-profit cannot be assumed to be more than $250. In the experience of Citizen Clinic, that spending is more likely to be closer to zero. Civil society organizations are no strangers to being starved for "overhead" costs,[9] and cybersecurity represents a significant expense for under-resourced organizations, as cybersecurity tools and services are not cheap. "Standard" tools like security keys, often credited by security experts as critical to stopping common attacks like phishing, range from $25–$50 each. If a security key alone consumes up to a third of an organization's per-employee digital safety budget, little will remain to administer and provide security capabilities, purchase secure storage, or buy and manage website security services.

There is a significant asymmetry between the resources of civil society organizations and their adversaries, particularly government adversaries. This means nonprofit defenders are likely to see diminishing returns on their investments in cybersecurity. Spending money to counter highly sophisticated threats is a tenuous proposition, particularly when the management of those new capabilities cannot be supported.

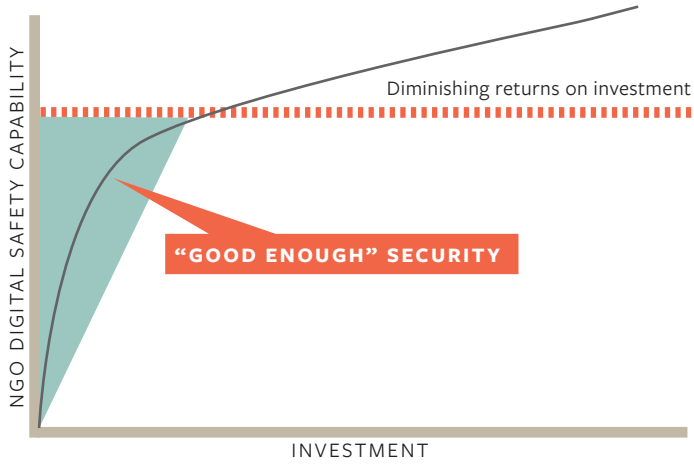

FIGURE 1: DIGITAL SAFETY INVESTMENT

Our work at Citizen Clinic has illustrated that many organizations have similar needs (albeit often with great nuance in implementation), with levels of security that place them in the "good enough" category (see Figure 1). "Good enough" security provides basic protections at a cost of time and money appropriate to the organization's budget, mission, and constraints. Beyond that, security investment is highly subjective to the risk posture of an organization. The threat of online attacks by a nation-state or other sophisticated actors requires dramatically different remediations deployed on an organization-by-organization basis, mitigations that are cost-prohibitive for the vast majority of NGOs.

8 Spiceworks. 2020. "The 2020 State of IT." https://www.spiceworks.com/marketing/state-of-it/report/

9 Gregory & Howard. 2009. "The Nonprofit Starvation Cycle." *Stanford Social Innovation Review:* https://ssir.org/articles/entry/the_nonprofit_starvation_cycle#

What needs to scale? The deployment of "good enough" security. Beyond that, organizations with particularly high risk profiles need to invest the time and energy into developing a risk-informed threat posture.

What Does Success Look Like?

The Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) provides a tiered description of cybersecurity implementation that serves as a useful model for measuring organizations' digital security.[10] Most CSO civil society organizations cannot be described accurately by Tier 1 ("Reactive"), rather they are starting at a Tier "0": they generally have no meaningful response to cybersecurity threats, nor the ability to respond to threats as they emerge. The first step in improving the digital safety posture of civil society often does not mean "hardening" organizational systems, it means helping overcome a perceived lack of agency. At Citizen Clinic, we've found that many organizations find cybersecurity to be such an overwhelming topic — the threats are too big, the subject matter too technical, the costs too high — that one of our core goals is to demonstrate to partners that a reasonably adequate level of online safety is possible with their current resources.

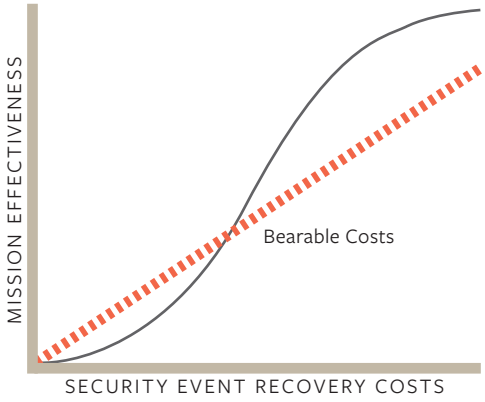

FIGURE 2: AS ONLINE EFFECTIVENESS GROWS, RECOVERY COSTS FROM POTENTIAL INCIDENTS INCREASE

The costs of a security incident do not have to be high to take many civil society organizations offline or permanently shut their doors. Given the deep importance of trust and legitimacy in civil society, costs can come in many forms beyond immediate financial loss: a drop in donor interest or lack of trust from a served community could be existential threats. However, many organizations are under pressure to publish, deliver services, or otherwise maintain a significant online presence. This pressure to increase online presence, often without incentives or support for security precautions, increases the likelihood (and potential) impact of a cybersecurity event. Improved security assistance needs to push civil society organizations to a point of resilience where they can withstand a basic attack, such as a device compromise resulting from an outdated operating system, or a DDoS attack on their website. Showing organizations the benefits of basic, low-cost security measures is often a critical step in generating buy-in.

10 Pg. 8 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Imagining Outcomes

Success depends on not just understanding how to improve an organization's capacity, but also the state of the ecosystem helping build that capacity, and the quality of their services. A variety of services are available in the technical assistance marketplace. Some are designed to meet the specific needs of organizations, others are geared toward improving the quality of the marketplace for cybersecurity services for nonprofits. The outcomes below are described with examples of specific tactics already used in the technical assistance ecosystem, along with examples from scaling efforts outside the cybersecurity space.

Quality of Service		Capacity Building		Ecosystem		
Contextually Informed	Responsive	Resilience	Confidence	Accessibility	Affordability	Assistance Networks

QUALITY OF SERVICE

Technical assistance can be structured in a variety of ways. Services may be provided holistically, or focus on a specific function, like emergency response, or a specific capability, like traffic management. Regardless of function, in order to achieve impact at scale, all technical assistance service providers should keep in mind a set of goals to ensure the quality of their service to civil society organizations.

In order to maintain high-quality service at scale, technical assistance must be both *contextually informed* and *responsive*. These goals can occasionally be at odds with one another, as the former requires a depth of relationship and knowledge that can dramatically slow the latter. However, without understanding an organization's context, technical assistance providers may not be able to know how to be effectively responsive. Answering baseline questions — what is the threat, where does it originate, who is the adversary, and what is the target organization capable of doing to address this threat — requires a strong grounding in the work of the organization. Responsiveness does not necessarily mean speed. It also means meeting organizations where they are and driving them toward meaningful capacity building.

Contextually Informed

The Center for Long-Term Cybersecurity's research on protecting politically targeted organizations online highlighted the importance of tailoring digital safety services to the specific missions and contexts of the communities in need. Citizen Clinic's service model — using multidisciplinary teams of students to form long-term partnerships with partners in civil society — was explicitly designed to address this challenge. Recommendations for organizational policies or technical controls that mitigate digital risks are vastly more effective and likely to be adopted if they are grounded in an understanding of an organization's priorities and values.[11] Thorough contextual assessment also enables technical assistance providers to understand the motivations and capabilities of threat actors, increasing the ability of providers to prioritize limited resources on mitigating attacker tactics that are both likely and of high potential impact on the mission priorities of the organization.

Learning From Practice: Citizen Clinic worked in partnership with another technical assistance provider to support a large international development accountability organization. Our partner assistance provider worked on a one-week contract to perform an in-office audit of the organization in question, and provided a detailed document identifying a number of technical, operational, and physical risks to their operations, and some potential mitigations. However, many of the recommendations — particularly those of a highly technical nature — were beyond the organization's ability to implement. Other recommendations, while following best practice, were not well-suited to the mission needs of the organization. Citizen Clinic teams followed up with the organization — with regular check-ins from our partner auditor — to custom-tailor policies, implementation guidance, and practices to help the organization address the critical risks documented in the audit. The resulting work took place over two semesters and is still ongoing at the time of this publication, and demonstrates the importance of long-term support informed by a strong understanding of the mission and practical working environment of the organization in need.

Another example of the importance of contextual awareness came early in Citizen Clinic's work. During one of our first client engagements, the Clinic deployed multifactor authentication (MFA) to three critical online accounts — email and two social networking services — and provided training to ensure staff knew how to manage and utilize the new login procedures. Six months later, a new student team from the Clinic evaluated that implementation, only to discover that the vast majority of the client's staff has disabled MFA. Upon inquiring further, Citizen Clinic learned that, due to the high likelihood of cellphone theft in their city, the client's staff were (correctly) afraid that losing their phone would lock them out of their accounts. While Citizen Clinic had presumed that an app-based authenticator would be the easiest choice for the organization, tying authentication to the client's phones was actually doomed to fail, not because of any technical barriers, but because of the broader context in which the client worked.

11 Section 2.3 of the SAFETAG framework, designed for risk-informed assessment of civil society's cybersecurity postures, explicitly details the importance of contextual awareness: https://safetag.org/guide/#section2.3

Established Tactics

1. **Assessment Frameworks:** Numerous assessment frameworks are available to help evaluate an organization's broader context. The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG), developed by Internews, is explicitly designed to assess digital safety risks to civil society organizations.[12] Citizen Clinic students also use the political, economic, social, technical, legal, and environmental framework (PESTLE) commonly used in the business world for developing a rapid understanding of the broad, often nuanced contexts in which NGOs work. This framework allows for all of the students' specialities — law, public policy, engineering, or otherwise — to contribute to the entire team's understanding of the client's context.

2. **Long-Term Partnership:** There is no good replacement for the understanding of the nuanced challenges facing an organization that can be gained through long-term collaboration. This is of particular importance when considering other organizational goals, like resilience and confidence capacity-building (more on this below). Organizations, their staffs, and their threat models change over time, and having a consistent, reliable partnership with a technical service provider can help targeted organizations prioritize investment in a productive fashion. Long-term partnership also affords the opportunity for monitoring and evaluation of implemented controls and practices, making it possible to refine tactics over time to help build a culture of security within the organization. While technical assistance need not be provided in perpetuity, having a consistent, reliable partnership can lower the time and money required for organizations to get support at a pace that is appropriate to their needs. As an example, Citizen Lab's long-term support of the Tibetan Action Institute allowed for the creation of the "Detached from Attachments" campaign, an effective community-based and contextually oriented campaign to resolve emerging threats to the Tibetan diaspora.[13]

External Examples

Mass customization is a significant mainstay of both the modern manufacturing and service economies. From architecture to fashion, industries have recognized that differentiating a

12 Internews "Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG): https://safetag.org/index.html

13 Satter & Bhatia. 2014. "Hacker-hit Tibetan monks 'detach from attachments'" *Associated Press:* https://apnews.com/df26c7f60abc449397b6c1deb7dccdd8

Learning From Practice: Citizen Clinic student teams often identify threats or issues that are common across our clients. However, the solution for one organization is rarely the best fit for all. A variety of contextual factors must be factored in, such as the organization's ability to pay for a new solution, the technical capacity of their staff, the reliability of their internet access, or even their politics, which might make the adoption of a specific software or platform's services untenable. Ignoring any of these variables carries significant risks for the Clinic's relationship with the partner organization. At best, it can result in ineffective recommendations; at worst, it can signal to a partner that the Clinic team does not appreciate the very real priorities dictated by the partner's mission. To accommodate this, Citizen Clinic maintains records about the services we provide to our partners *and the rationale for the recommendation* so that future student teams can leverage the product research and implementation methods of past teams, while still ensuring the assistance they provide is justified by the partner's specific needs.

For example, many Citizen Clinic teams have performed phishing training for our clients. We have standardized both our technical infrastructure and our organizational design and policies around how to run these exercises, but to be effective, each deployment must still be tailored to the specific client in a way that takes into account their organizational missions, risks, and adversaries.

common set of services to meet the specific needs of individual customers vastly increases the market for those services.[14] By pushing that customization as far down the supply chain as possible, service providers can maximize their audience but keep costs controlled. Most mass-customization is facilitated by algorithmic capabilities, but many businesses, such as the custom fashion subscription service StitchFix, leverage modern supply-chain capabilities combined with human specialists to offer custom services at scale.

The needs of targeted civil society organizations may be similar across many contexts — we have found secure communications, safe digital storage, and online reputation management to be common challenges — but each organization's context dictates nuanced differences in what products, services, or policies are the best fit. As in other fields, wealthier customers can generally afford a greater level of customization, while affordable options are more generic. But delivered effectively, mass customization can help reduce the significant asymmetry between civil society organizations and their adversaries.

At the other end of the supply chain, **specialization** can be a powerful tool for addressing the needs of smaller communities of interest that may have more consistent needs than the whole of a sector. Law clinics have grown substantially in their maturity since their invention half a century ago, and are now consistently specialized in specific areas of legal practice, such as

14 Gilmore & Pine. 1997. "The four faces of mass customization." Harvard Business Review, vol. 75, no. 1.

environmental law, death penalty cases, or immigration. Specialized digital safety services are emerging as well: a clinic at Cornell Tech, for example, focuses on protecting the survivors of domestic abuse;[15] and a technical assistance fund focuses on serving reproductive healthcare providers and advocates.[16]

Responsive

Many civil society organizations operate in high-risk environments where emergencies can arise. Rapid response to digital safety incidents can make a meaningful difference in protecting organizations' reputation and the physical and psychological dangers that might stem from online attacks. CLTC's past research has found that rapid-response efforts made up a disproportionately large number of overall technical assistance efforts. Because many organizations face significant capability asymmetries with their online adversaries, incident response and recovery efforts are a critical component in supporting their security.

Established Tactics

1. **Rapid Response:** A number of resources are available to help organizations respond to emergencies, including the AccessNow Digital Security Helpline and the RaReNET/CiviCERT program.[17] These programs provide immediate support for organizations that are under immediate attack. While digital security helpdesks offer an array of services, they generally deliver staff support and ecosystem activation. Targeted organizations generally do not have the expertise to detect, resolve, and document online security incidents, nor are they capable of realigning their systems to ensure the same type of attack does not happen again. Emergency response programs offer the services of skilled practitioners to help identify and resolve attacks, and can leverage a trusted network of external experts to assist in the recovery process. These networks are often informal, however, which presents a major barrier to scale. As an added challenge, many organizations do not contact rapid response programs until they are confident they are in the midst of an emergency, leaving many precusor incidents (such as suspicious emails) undocumented.

15 Havron, et. al. 2019. "Clinical Computer Security for Victims of Intimate Partner Violence" Cornell Tech, New York University: https://www.cs.cornell.edu/~havron/pubs/clinicalsec.pdf, Clinic to End Tech Abuse: https://www.ceta.tech.cornell.edu/

16 Digital Defense Fund: https://digitaldefensefund.org/about/

17 Access Now Digital Security Helpline: https://www.accessnow.org/help/ and CIVICERT: https://www.civicert.org/

Learning From Practice: In 2019, a Citizen Clinic client (Org A) alerted us to a posting on a major social media platform. The posting indicated that someone had gained access to private emails between their staff and another organization (Org B) in Latin America. The emails were being used to harass and spread misinformation about both organizations. While Citizen Clinic is not an emergency response organization, we worked with Org A to track the spread of misinformation by leveraging our network in the research community to identify suspicious and potentially inauthentic behavior. Clinic staff also worked with Org A to ensure their systems had not been compromised, and even communicated with Org B in Latin America to provide advice on how to manage potentially compromised accounts. Citizen Clinic was able to provide additional information directly to the social media platform in question, and we referred Org A and Org B to additional support resources. However, because Org B in Latin America was not our direct client, the Clinic was limited in the amount of direct support we could provide.

While this process is not a core competency of the Clinic, the experience highlights that responsiveness is a critical capability for all technical assistance providers. The reputational attack on our client was minor, resulting in only a few thousand online postings over a two-week period, but it presented a significant threat to the legitimacy of their work in the region. Members of our network of technical assistance providers, researchers, and private-sector actors all played different roles in the resolution of this issue, and our work with our client continues today. We were also able to leverage our relationships to find a Latin America-based technical assistance provider to help Org B receive more local, long-term support than Citizen Clinic could provide.

2. **Ecosystem Activation:** Some organizations, such as CiviCERT or the Center for Digital Resilience, exist explicitly to facilitate the activation of different ecosystem players.[18] Formalizing these channels has a number of advantages. Relationship-based models exclude many civil society organizations that do not have connections to the digital rights space, most of which is based in the Global North. As a result, segments of global civil society most likely to be targeted by substantial surveillance or online attacks are least likely to have access to the trust relationships necessary to facilitate rapid response.

While projects like CiviCERT have formalized some of these channels, additional or broader formal channels could provide on-ramps for additional players to join the rapid response ecosystem. Many of the technical assistance providers in the rapid response space are NGOs themselves. Many major private-sector technology platforms also have teams to help high-risk users with security, privacy, trust, and safety. However, these teams often have neither the bandwidth nor the reach and trust with civil society necessary to manage new relationships with organizations requiring emergency assistance. To bridge this gap, private firms can develop informal relationships with cybersecurity experts in civil society, but this requires time

18 Center for Digital Resilience: https://digiresilience.org/

and resources, and not all civil society security experts have the ability to vet a new platform or corporate entity as a partner. Establishing formal channels for these relationships can help private-sector firms provide assistance to targeted civil society groups.

External Examples

While many emergency support organizations have historically operated from an international level, pushing support out to specific regions or organizations in need, a growing number of service providers offer support locally. Providing regional or community-specific support for organizations in need decreases start-up time and lowers barriers to access. It also helps with understanding context, and makes support infrastructure more adaptive. There are of course inefficiencies in "cell" structures that prevent decentralized organizations from benefiting from some economies of scale, but they are also more capable of surviving an attack or organizational setback, as each local entity is designed to operate with a high level of independence.[19]

Decentralization, or managing an organization or project in a manner that is remote and non-hierarchical, with limited centralized leadership, has become a hallmark of internet-enabled civil society, as it allows independent activists and organizations to collaborate across political boundaries for collective action. This trend introduces security risks (via communications technologies), but, with the right guidance, can also create opportunities for data redundancy or leveraging the patchwork quilt of data protection laws in a way that protects organizations' operations. Given the limited number of skilled technical assistance providers, decentralization is likely key to meeting the needs of civil society organizations, particularly in regions and communities with more limited access to digital safety expertise. This requires a greater proliferation of localized organizations that have direct reach to both communities in need *and* the technical assistance ecosystem.

BUILDING CAPACITY

Direct support and partnership are both important for improving the security of civil society organizations, but external help can only go so far. Truly scaling technical assistance requires

19 The importance, and agility, of locally-informed assistance can be seen in Afghanistan, where the Taliban has grown legitimacy and popular support due to their ability to resolve local disputes with greater speed than the central Afghani government. Constable. 2018. "The Taliban has Successfully Built a Parallel State in Many Parts of Afghanistan, Report Says" *The Washington Post:* https://www.washingtonpost.com/news/worldviews/wp/2018/06/21/the-taliban-has-successfully-built-a-parallel-state-in-many-parts-of-afghanistan-report-says/

helping organizations build their capacity to manage a certain level of digital safety risk on their own. Capacity building can help organizations improve their internal resilience and confidence in a way that is sustainable over time.

Resilience

Cybersecurity technical assistance should not merely seek to resolve existing vulnerabilities, but rather should improve an organization's resilience to cyberattacks over time. This can be challenging, however, as few organizations have the capacity to hire internal technical experts to manage digital safety issues with the ongoing attention they deserve. Past technical assistance efforts have illustrated that improving technical skills for employees in low-resource contexts can accelerate the departure of those employees for higher paying jobs.[20] However, with the cybersecurity workforce already too small, it is unlikely that civil society organizations will be in a position to make competitive hires any time soon. Therefore, technical assistance providers must both teach the critical thinking skills necessary to plan and manage baseline security concerns, as well as the technical skills necessary to implement and maintain security solutions over time.

Established Tactics

1. **Policies you can "turn on":** Many civil society organizations lack basic security policies and processes, at a general level and for specific processes like data management, incident response, and international travel. Many policy templates only offer legalistic/liability protections, instead of actionable frameworks for assigning tasks and prioritizing resources.[21] Some products offer administrative controls, such as the ability to view and edit Google or Microsoft account permissions broadly, but many of these products require more expertise or time than many low-resource organizations have available. Products that enable more robust technical controls, such as mobile device management solutions, are often out of reach financially and technically for targeted organizations. Some capabilities, like

20 Birdsall, Nancy. 2007. "Do No Harm: Aid, Weak Institutions, and the Missing Middle in Africa," Working Paper Number 113. Center for Global Development.

21 For example, the SANS Institute publishes a variety of template information security policies here: https://www.sans.org/security-resources/policies/. However, most of these templates are legalistic in nature, and do not give much guidance to organizations on how to task ownership and management of various security activities within an organization.

Google's Advanced Protection Program or EFF's LetsEncrypt project, substantially lower the barriers to accessing better protections for individuals and organizations. But significant work still needs to be done to profile or template settings for common services so CSOs can easily turn on high-security settings and have confidence in their ongoing safety.

2. **Set and forget (for a while):** While persistent monitoring can be a challenge, many common security controls do not require ongoing maintenance. Enabling HTTPS on organization-owned websites and services, forcing multi-factor authentication on organization-owned accounts, and changing website login addresses to a unique URL are all examples of controls that require a lower amount of effort but can result in long-term improvements to organizational security. These are not permanent solutions — security certificates must be kept up to date, and MFA tokens must be purchased and replaced when lost — and some controls, like signing up for a DDoS mitigation service, even at great discount, require some technical sophistication to enable. But these security measures are "low-hanging fruit" that can improve security while allowing organizations to focus training and resources on longer-term, customized efforts.

External Examples

In other fields, tasks once thought to be solely the domain of experts have been increasingly **transferred to more junior or less-expert staff** as the work becomes increasingly standardized or predictable. In the legal field, for example, the role of paralegals has expanded significantly, and junior-level attorneys often provide legal services that were once reserved for more senior lawyers.[22] The nurse practitioner role in health care similarly has taken on more responsibility as the field has come to recognize the impracticality of having routine medical assessments, care, and procedures performed by more specialized medical doctors.[23]

While the cybersecurity field at large is in dire need of junior-level talent, many of the security tasks currently handled by non-profits' directors of operations or system administrators could be managed by junior staff members. There *is* a risk of overburdening technology staff in low-resource organizations by adding more technical responsibilities to their portfolio. As many of the standard needs of NGOs do not require advanced technology skills to administer, junior-level program staff at non-profits could see some of these tasks integrated into their

22 Mongue. 2017. "From Apprentice to Paralegal: The Rise of the Paralegal Profession in America" Issues in Legal Scholarship" https://doi.org/10.1515/ils-2016-0261

23 Laurant, et al. 2018. "Nurses as substitutes for doctors in primary care." Cochrane Database Syst Rev.

responsibilities. Multiple Citizen Clinic client engagements have resulted in identifying and assigning junior- or mid-level staff members to take leadership roles in managing specific security tasks, such as onboarding and auditing the use of MFA on critical accounts, reviewing and managing storage permissions, and managing on- and off-boarding of new staff into organization-owned services like email, relationship management (CRM) systems, etc.

Low-level staff at public-interest organizations are often responsible for ongoing processes to facilitate their programs' needs, including communications, grant reporting, and project management. Empowering junior staff to own some basic security responsibilities could help engender the public-interest sector with a growing appreciation for these tasks. As a note of caution, Citizen Clinic (and many others) have found that executive buy-in is a critical component of successful capacity-building. It is not enough to merely task junior staff with security responsibilities; they must be enfranchised with authority to ensure protocols are followed by more senior staff.

Automation of repetitive or predictable tasks can additionally help organizations improve the sophistication of their security practices. A number of productivity tools — from task management to meeting scheduling — increasingly rely on automation to remove some of the "busywork" of repeatable tasks. Cybersecurity artificial intelligence and machine-learning products offer some automation opportunities for enterprise customers, but the outputs from these products still require a high degree of expertise and time. Additional automation, particularly for network security and mobile device and permission management, could have dramatic benefits for civil society organizations trying to manage security, but only if the developers of the technology significantly limit or eliminate the client-side management required.

Confidence

Digital safety risks are intimidating, not only because of the dangers they present both online and off, but also because of the insidious nature of being attacked in an always-connected work environment in ways that can be difficult to detect, or with a tide of overt harassment that seems impossible to stem. In order to embrace the operational overhead that comes with managing digital risks, CSOs must feel confident they can make a difference.

Established Tactics

Establishing Ownership: There is a significant amount of focus in security on how individuals contribute to the security of a system. However, individuals in public-interest organizations are stretched thin. While individual (and leadership) buy-in is critical to the success of securing an organization, assigning ownership over specific security controls is critical to ensuring adherence to policy and ongoing administration of technical protections. For example, many partners of Citizen Clinic have requested security plans or procedures for travel, incident response, or other organizational needs. Assigning individuals to become "owners" over specific controls can help ensure they are maintained.

Learning From Practice: Multiple Citizen Clinic partners have struggled with secure permissioning on cloud-based file storage services like Google Drive or Dropbox. While those services provide security benefits, access control to documents can be difficult to manage over time. Particularly in organizations with significant volunteer contributions or staff turnover, a lack of oversight on detailed permission structures can expose information and create undue risk.

Clinic students have used a number of different strategies to audit and develop solutions for cloud storage permissioning, including developing crosswalks between staff responsibilities and document content. Tiering access to files (following the classic principle of least privilege) is one way to manage permissions, but someone must be in charge of ensuring those tiers remain relevant to the operational reality of the organization. Reorganizing a partner's data storage is one step, but just as critical is empowering a particular staffer to maintain that new storage integrity. Clinic students have trained executive directors, operations managers, project leads, and junior staff on how to manage specific segments of organizational file structures. This allows for plans and policies that assign specific owners for permission management, establish timelines for review of those permissions, and develop accountability mechanisms based on those timelines.

1. **Learning how to ask the right questions:** The digital security landscape changes rapidly. Staying abreast of new threats, controls, and practices is a time- and energy-consuming task beyond the scope of the responsibilities, time, and expertise of many public-interest professionals. The swift pace of change in the space can feel overwhelming, leading many politically targeted organizations to feel helpless about digital safety. But creating *expertise* is not the goal of technical assistance. Recipients of security assistance should feel empowered to understand their risk context, including what types of threat actors they face, what vulnerabilities they may have exposed, and how (and to whom) to escalate questions as they emerge.

External Examples

Many international development programs have worked to improve the confidence of individuals or local programs to address critical needs. Some have been focused on individuals, such as financial inclusion models designed to empower women to gain independence.[24] Others have looked at improving capabilities at a community level, such as expanding the ability of community health volunteers to take on additional responsibilities.[25] Not all of these have been successful, but there is evidence that, just as some expert-level tasks can be distributed to less-trained staff or volunteers, individuals can be empowered to take on tasks that were once considered out of their reach. But that transfer of responsibility requires confidence-building, not mere training, to ensure ownership.

ECOSYSTEM

While scaling up the delivery of support is critical, technical assistance providers must find ways to enhance some critical components to ensure their own health. This section reviews three outcomes — accessibility, affordability, and support structure — that can increase the impact of technical assistance programs across the entire spectrum of civil society organizations.

Accessibility

Established Tactics

1. **Culturally Informed Support:** Just as technical assistance providers should contextualize support for their clients, organizations should develop messages that are culturally relevant to ensure they resonate with their broader communities. As a well-known example, Citizen Lab partnered with Tibet Action Institute to develop the "Detached from Attachments" campaign, which used Tibetan cultural and humor cues to coach the broad diaspora to move away from email attachments. At the time, attachments were the primary vehicle for Chinese state malware targeting the diaspora, and the campaign helped users learn to

24 Barasa & Lugo. 2015. "Is M-PESA a model for financial inclusion and women empowerment in Kenya?" Contemporary Global Perspectives on Gender Economics. https://www.igi-global.com/chapter/is-m-pesa-a-model-for-financial-inclusion-and-women-empowerment-in-kenya/134133

25 Lamichhane. 2019. "Female health volunteers of Nepal: the backbone of health care." Lancet.

distrust attachments at a time when cloud-based file sharing was still relatively rare. Understanding the specific threats and cultural cues that will help transmit knowledge is key to providing broader support.

2. **Regional and Subject-Matter Expertise:** Our previous research into the technical assistance ecosystem for civil society cybersecurity illustrated that many of the existing assistance providers are civil society organizations themselves. While this creates limitations on the range of assistance available, many technical assistance organizations have emerged from within specific communities of need. Organizations like the Digital Defense Fund[26] have emerged to provide digital safety services to organizations within the reproductive rights community, offering a range of support specifically tailored to that audience, and building on a trust network that comes from sustaining relationships over time. The Center for Digital Resilience provides a service to match civil society organizations with local security practitioners, ensuring that even if the organization in need is not a sophisticated consumer of security products, it can access a provider with the knowledge and skills to help them.[27] Providing support to specific communities of interest substantially lowers the start-up costs of engagements, improves the quality of service, and engenders trust relationships that endure beyond specific projects.

External Examples

Much as pushing expert practice down the organizational ladder helps organizations scale their response to problems, it also improves the state of the ecosystem by creating new job opportunities with fewer educational and experience boundaries, moving more people into the field. Expert practitioners are then freed up to examine more complicated problems, improving the state of research and high-level practice. Given the dearth of public-interest cybersecurity providers, **finding new pathways for onboarding less-experienced professionals into the space** is critical to providing more helping hands.[28]

When civil society organizations have a digital safety problem, they may not know where to turn for support. **The lack of known, approachable pathways** for support continues to be a barrier. Even cybersecurity guides — many of which litter the internet — are rarely translated out of English. Localization Lab, a decentralized network with over 6,000 members,

26 https://digitaldefensefund.org/
27 https://digiresilience.org/
28 Brooks, *Defending Politically Vulnerable Organizations Online*

provides free translation/accessibility services for software, technical documentation, and even cybersecurity guidance, helping transform technical literature into more broadly readable documentation.[29]

Affordability

Civil society organizations' ability to engage in the cybersecurity marketplace is significantly limited by their financial resources. Therefore, affordable security products and services are critical to helping organizations become informed security customers.

Established Tactics

1. **Lowering Cost Barriers:** This is one of the more established tactics for scale, and many products and services exist to improve general access to certain aspects of digital security. For example, DDoS attacks — once a significant concern for organizations and businesses alike — have been all but nullified by the emergence of content delivery networks like Cloudflare. Programs from private-sector providers, like Cloudflare's Project Galileo[30] and Google's Project Shield,[31] and public-interest projects like eQualitie's Deflect[32] platform, all offer free DDoS protection to non-profits. In general, web security has improved dramatically in recent years, with website construction services like Wordpress and Squarespace offering easy toggles for difficult-to-configure services like HTTPS. Similarly, the proliferation of end-to-end encryption on major communications platforms like Whatsapp has enhanced security for end-users, and the success of user-friendly design in more purpose-built security products like Open Whisper Systems' Signal messenger make strong encryption far easier to access.

External Examples

Starting in the early 2000s, the **availability of cardiopulmonary resuscitation (CPR) training** began to rise as the medical community advocated for more widespread education

29 Localization Lab https://www.localizationlab.org/
30 Cloudflare Project Galileo https://www.cloudflare.com/galileo/
31 Google Project Shield: https://projectshield.withgoogle.com/
32 eQualitie Deflect: https://equalit.ie/portfolio/deflect/

on how to conduct the life-saving procedure. Similarly, improved design of automated external defibrillators (AEDs) nearly eliminated the potential for erroneous shock, and significantly increased the chances that a victim of a cardiopulmonary event would survive. In the last 15 years, both CPR training and AED kits have become increasingly common. Deployment of the CPR and AED kits is not the only benefit, though, as research has shown that the accompanying training helped individuals recognize signs of distress and improved the rates of calls for assistance, greatly improving victims' chances of receiving urgent care.[33]

Government agencies have seen significant cost savings since the adoption of **shared services models** for IT procurement and development, and shared technology infrastructure has saved the U.S. federal government tens of billions of dollars over 10 years, according to estimates.[34] Given the increasingly decentralized work of many civil society collectives, sharing technology investments could not only provide sizable cost savings, but also allow the groups to collectively gain access to "enterprise-class" security offerings not available through "non-profit-level" services.

Assistance Networks

Maximizing effective distribution of work among technical assistance providers — whatever model they utilize — is critically important, given the breadth of need. Such workload rebalancing can be achieved through international collaboration, expert activation, or even project management. But the expansion and improved functioning of the networks connecting providers will be critical to improving the health of the broader ecosystem providing security assistance.

Established Tactics

1. **Emergency Response Networks:** A number of digital emergency response networks exist, some with the ability to deploy resources internationally to help organizations find local support in resolving digital threats. Services like AccessNow's Digital Security Helpline[35] and Frontline Defenders' emergency contact line[36] provide rapid support for organizations in

33 Cave, et al. 2011. "Importance and Implementation of Training in Cardiopulmonary Resuscitation and Automated External Defibrillation in Schools.", American Heart Association Emergency Cardiovascular Care Committee. https://www.ahajournals.org/doi/10.1161/CIR.0b013e31820b5328

34 Shared Services Roundtable. 2015. "Building a Shared Service Marketplace." Partnership for Public Service: https://ourpublicservice.org/wp-content/uploads/2015/03/9c8950a6070174ec3881895399509c72-1425334250.pdf

35 AccessNow Digital Security Helpline: https://www.accessnow.org/help/

36 Frontline Defenders Emergency Contact: https://www.frontlinedefenders.org/emergency-contact

need. While these services are limited, having a reliable point of contact in an emergency is a vital support to organizations under attack.

2. **Human Capital:** Citizen Clinic and other members of the Public Interest Technology University Network are actively training young professionals with the skills necessary to engage with civil society organizations on technology issues. Citizen Clinic has found that the public-interest opportunities offered by our program draw a broad range of students toward the field, including students from non-technical backgrounds and technically trained students who previously felt cybersecurity was "not for them." Such educational programs can create a long-term pipeline of talent to serve the public-interest sector.

Learning From Practice: The connections that Citizen Clinic, Access Now, and other technical assistance providers bring to relationships with civil society organizations are of critical importance. Personal, trusted relationships with security, privacy, and trust and safety teams at major technology platforms can allow technical assistance providers help their partners receive expedited support on issues ranging from account takeovers to targeted harassment. However, the structures of these relationships are inherently undemocratic; only organizations and individuals with connections to established technical assistance providers get access to those trusted support pathways. While formalizing these pathways might seem like an obvious solution, many platforms face barriers: the attackers may be governments (creating liability concerns), not all requests are legitimate (technically or otherwise), and the workload for the higher-level security practitioners who serve as points of contact for assistance providers in those organizations creates new problems of scale.

Major technology platforms and service providers must continue to find ways to establish trustworthy channels for getting input from civil society organizations under attack. Technical assistance providers and networks can be a way to vet requests, but these providers do not want to simply push information about their partners in civil society to companies and hope for fair adjudication. Those providers need a feedback loop so they can provide the most effective support to their clients and partner NGOs. At Citizen Clinic, we have heard from many technology platforms that, while they are happy to help curtail bad behavior on their platform, they will not provide the Clinic with information about the attackers. This makes sense, given the sensitivity of the information, but limits how well Citizen Clinic and other assistance providers can help clients recover after an attack. The controls we might recommend to a client who has been attacked by a government, for example, differ significantly from those we would recommend to those attacked by a hate group. Outside the walled data gardens of the technology platforms, it is often impossible to understand the full nature of a threat.

Citizen Clinic teams have also engaged with multiple experts on the cutting edge of new digital safety techniques. Some teams have worked with Tall Poppy — a startup focused on mitigating digital harassment threats to organizations and their high-profile staffs — to understand emerging harassment and disinformation defenses, and to help clients adopt these techniques.[37]

37 Tall Poppy: https://tallpoppy.com/

External Examples

1. The **cybersecurity insurance marketplace** is still in its infancy, but an outgrowth of offerings dedicated to supporting non-profits or small businesses could substantially help resource-constrained organizations survive a serious cyberattack. Not only could insurance offer a financial backstop, but it could incentivize organizations to embrace more robust risk-management practices, much as businesses must demonstrate to insurers a good-faith effort to manage risk. While getting civil society organizations to buy cybersecurity-specific insurance is a tough sell, technical assistance providers may want to explore how their partners' existing insurance (such as business interruption or property and casualty insurance) could serve as a "silent" cybersecurity insurance policy, covering many of the risks organizations are concerned about. Most organizations do not have cybersecurity insurance yet, however, as many property and casualty insurance policies have exceptions for online criminal events, and those interested in purchasing cyber insurance often do not know how much to buy.[38]

38 Deloitte Center for Financial Services. 2017. "Demystifying cyber insurance coverage". Deloitte University Press. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-demystifying-cyber-insurance-coverage-report.pdf

Exploring Solutions

Next we explore potential mechanisms for improving the scale of digital safety technical assistance. This section provides a high-level view of existing technical assistance models that have emerged in recent years to expand the availability of digital safety services. We do not intend to suggest that any of these options is better than others, but rather to help technical assistance providers, funders, and beneficiaries of digital safety support better assess if a particular model may work well for their needs. Figure 3 summarizes the performance of three models for technical assistance across the seven outcomes defined in the previous section.

	Quality of Service		Capacity Building		Ecosystem		
	Contextually Informed	Responsive	Resilience	Confidence	Accessibility	Affordability	Assistance Networks
Volunteer Networks							
Digital Safety Clinics							
Community Hubs							

FIGURE 3: In this figure, green signifies this outcome is a core competency of the model, while blue highlights outcomes that are clearly benefited by the model. If a field is colorless, that does not mean a model provides zero benefits in pursuit of this outcome, but rather that it is not an obvious match. As all of these models are still new, new hybrids and experiments could emerge that change the descriptions in this document.

VOLUNTEER NETWORKS

Digital safety volunteer networks come in many forms: informal or formalized, community-based and international. In our work at Citizen Clinic, we have encountered an array of volunteer efforts aimed at providing cybersecurity support to civil society organizations. Most networks comprise cybersecurity professionals who coordinate their work by email, Slack, or word of mouth. Some volunteer efforts are highly decentralized and rely on crowdsourcing and funding, while others — including I Am the Calvary, The Global Cyber Alliance, and the Cybercrime Support Network — rely on coordinated expert contributions. However, few of these volunteer networks explicitly serve NGOs at risk from politically motivated attacks.

Cybersecurity has a number of diverse fields of practice (network security, application security, data protection, privacy, trust and safety, etc.), and creating a network of experts to provide help to CSOs could offer significant benefits. Leveraging experts on a decentralized basis and

connecting them with communities or individuals in need is not understood, though some research from other domains offers guidance. For example, a 2014 study of online expert networks in the medical community showed benefits from connecting doctors with one another to share best practices and new research across medical disciplines.[39] However, that study also illustrated many potential challenges: medical professionals reported the network was helpful, but potentially distracting. While the network helps scale the availability of information, it does not necessarily scale the number of practitioners or organizations' access to those experts.

Volunteer expert networks also do not necessarily improve security outcomes beyond "good enough." Experts can help higher-risk organizations respond to a crisis or fend off sophisticated attacks, but do not build NGOs' digital safety capacity over time. As a result, volunteer efforts must be closely monitored to ensure their quality and long-term impact, as expert volunteers may not have experience with the nuances of supporting civil society. These nuances include political, cultural, and social issues that create a different moral framework about technology choices (such as whether to support the "surveillance capitalism" business model of advertising-based online services); communications (the use of appropriate pronouns, the pace of communications, and acceptable humor); and organizational priorities (driven by motivations beyond profitability, uptime, or other metrics used by the private sector to define success). Oversight of volunteer efforts could come in many forms, but without a well-established feedback loop, it will be hard for supported organizations to voice complaints or evaluate the effectiveness of the service they received.

While volunteer networks may not build capacity in the same way as a more tailored, one-to-one assistance project, they can be incredibly responsive to emerging needs. The Global Threat Alliance created a "work from home" guide for organizations forced into remote work due to the COVID-19 outbreak.[40] And I Am the Calvary developed a model that allows their volunteers deep, trusted access to sensitive public infrastructure in need of improved security.[41] There is a clear desire among security professionals to expand the availability of digital safety skills outside the boundaries of their day jobs, and volunteer networks may have untapped potential for improving the state of the ecosystem.

39 Crowdsourcing medical expertise in near real time - Sims - 2014 - Journal of Hospital Medicine

40 https://workfromhome.globalcyberalliance.org/

41 https://www.iamthecavalry.org/domains/infrastructure/

	Quality of Service		Capacity Building		Ecosystem		
	Contextually Informed	Responsive	Resilience	Confidence	Accessibility	Affordability	Assistance Networks
Volunteer Networks		Access to more experts to respond to emergent issues			Potential new service access through trusted and capable practitioners	Volunteers can offer free or heavily discounted services	

DIGITAL SAFETY CLINICS

Citizen Clinic and other university-based clinics address many of the challenges of scale in a cost-effective way. Digital security clinics follow the model of law and medical clinics, which expand access to needed services while providing students with experience and practical knowledge, better preparing them for the workforce and creating an on-ramp to public service work. Clinics can specialize and build deep ties with communities, draw from the student body's diversity, experiment with new methodologies in a rigorous manner, and provide questions for technical and non-technical researchers to pursue outside the clinic.

Clinics do have limitations, however. Student labor is, by definition, less professional and experienced and requires supervision and space for failure (along with backstops to prevent those failures from reaching clinic beneficiaries). Student work is also confined to the academic calendar which, while predictable, limits most engagements to those that can be scheduled on a regular cycle. Students must balance clinic coursework with many competing priorities outside their clinic class. The model is also very new, even compared to other technical assistance methods in this space, so additional drawbacks may still yet emerge. And any single clinic is unlikely to deliver significant scale to technical assistance. Much like law clinics, scaling digital safety clinics depends on many universities adopting the model, specializing, and further developing the discipline of practice. Universities, however, must staff clinics with experts to supervise and educate students, requiring funding that is not readily available.

	Quality of Service		Capacity Building		Ecosystem		
	Contextually Informed	Responsive	Resilience	Confidence	Accessibility	Affordability	Assistance Networks
Digital Safety Clinics	Opportunity to draw from diverse student backgrounds		Clinic projects can be designed to tackle longer-term problems	Direct support and relationship building improve org and provider capabilities	Improves access to technical assistance and an on-ramp for new professionals	Clinic services are traditionally free or highly subsidized	Academic institutions provide significant staying power for student cohorts and clients

COMMUNITY HUBS

At this point, community hubs — organizations designed to provide digital safety services to specific communities in need — are an understudied model[42] for providing technical assistance to civil society, but anecdotally they offer compelling potential. By situating a technical assistance organization within a community of interest, many of the challenges of understanding context are alleviated. Such hubs can move swiftly to provide direct technical assistance with relatively few startup costs, and can manage both capacity-building projects and emergency response efforts.

Existing community hubs for cybersecurity expertise have adopted a variety of models, including formal organizations and volunteer-led efforts. The Digital Defense Fund provides digital safety support for a large range of reproductive rights advocates, support networks, and healthcare providers in the U.S., and maintains a full-time staff and a broad network of partners. Other organizations, like Karisma in Colombia, R3D in Mexico, or the Electronic Frontier Foundation in the U.S., are primarily digital rights advocates, whose expertise often leads them to provide technical assistance to members of their immediate communities. There is no single model for a community hub, but the value proposition relies on a professional, experienced, contextually informed staff providing support to a community they know well.

There are drawbacks to this model. These hubs are expected to be "everything to everyone" in their communities, as they are asked for support on issues ranging from sophisticated,

42 While there are not specific studies on this form of assistance, plenty of work on community-oriented health, research, security and policing, and other fields suggest this model is likely to bear fruit across many different contexts. This report from NESTA suggests that patient organizations not only improve capacity and knowledge across a community of interest in need of healthcare, but also yields insights about care provision unique to the model: https://www.nesta.org.uk/report/collective-intelligence-in-patient-organisations/

targeted attacks, to network security, to basic software selection. Some have even taken on the role of grantmaker in order to support their communities' efforts to procure and deploy needed software and services. But this level of support can be difficult to maintain, particularly with a small staff likely making less money than they would in the private sector with similar responsibilities. It is also not immediately clear how to set up centers for technical assistance within communities that do not already have a core of expertise in the field. If philanthropies wish to support a community-centric model for expanding the ecosystem, they will need to explore models for kickstarting a project from within that community. At this stage, it remains unstudied how funders can best support community leadership to take on this role, but as illustrated elsewhere in this document, there are many analogies (and cautionary lessons) from the international development field.

	Quality of Service		Capacity Building		Ecosystem		
	Contextually Informed	Responsive	Resilience	Confidence	Accessibility	Affordability	Assistance Networks
Community Hubs	Already embedded in context	Close community ties shorten response time	Improves general knowledge and can communicate emergent best practices across partners	Can serve as a stable, enduring partner for the long-term with community orgs			Can serve as a point of contact for other providers, companies, etc. who want to support a community

Conclusion

The three technical assistance models examined in this report all provide different potential benefits, but all contribute differently to scaling digital security services for civil society organizations. The future will require innovation and experimentation to develop models and communicate about the risks to policymakers, technology firms, funders, researchers, and senior leaders in civil society. Activating already existing expertise and helping organizations utilize existing channels for support is an important element, but we must also expand the number of professionals in the space. A more nuanced perspective on the digital safety challenges facing civil society organizations is essential not only for providing a high quality of service, but also for designing appropriate technical products and policies.

It is possible for civil society organizations to achieve "good enough" security that makes a difference in their online safety, but more substantial shifts are necessary to address the market needs for civil society security at scale, and at pace, to match the need. This paper lays out the objective functions that the market shifts need to solve for by describing seven outcomes of improved assistance at scale. The future of the space will require innovation and experimentation to develop models that embrace, combine, and network these capabilities.

Eva Galperin's groundbreaking work to support the victims of intimate partner violence illustrates how existing models can form an ecosystem of support that is more than the sum of its parts. With support from security researchers at the Cornell/NYU cybersecurity clinic for survivors of intimate partner violence[43] and volunteer researchers at the security firm Kaspersky, Galperin has taken a serious chunk out of the stalkerware industry that enables abusive partners.[44] She has also contributed to Callisto, a project to faciliate a survivor community-created system for detecting repeat perptrators of sexual violence.[45] These projects leverage expert volunteers, a university-based clinic, and community-centric support to create an ecosystem of assistance for survivors of intimate partner violence that addresses the problem of technology-enabled abuse like never before.

43 Computer Security and Privacy for Survivors of Intimate Partner Violence: https://www.ipvtechresearch.org/, and Clinic to End Tech Abuse: https://www.ceta.tech.cornell.edu/

44 Greenberg. 2019. "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware" *Wired:* https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

45 Project Callisto: https://www.projectcallisto.org/

Community-engaged providers can work from the ground up to address the evolving threat landscape. Technology platforms and providers can provide assistance, and governments can compel certain security, safety, and privacy-enhancing design decisions. But policy and products designed to serve the social good must be responsive to the requirements articulated by an active, connected, and high-functioning set of digital safety experts who are deeply engaged with civil society on a regular basis.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley