Ties That Bind

Organisational Security for Civil Society

Executive Summary

Prepared by The Engine Room for the Ford Foundation
March 2018

THE
ENGINE
ROOM

This research report, commissioned by the Ford Foundation, was conducted by The Engine Room from January-December 2017. The content of this report does not reflect the official opinion of the Ford Foundation, and responsibility for the information and views expressed in the report lies entirely with The Engine Room.

Commissioning Editors and Content Support: Michael Brennan, Jean Cook, Ryan Gerety, Jenny Toomey.

Lead Researcher: Zara Rahman (The Engine Room)
Research Assistant: Paola Verhaert (The Engine Room)
Research and Content: Nicole Anand, Alix Dunn, Laura Guzman, Anca Matioc, Maya Richman, (The Engine Room)
Illustrations: Jason Li, http://hongkonggong.com/
Report Design: Adjoa Opoku

The Engine Room requests due acknowledgement and quotes from this publication to be referenced as: The Engine Room: Strengthening The Digital Security Support Ecosystem, March 2018. This report is available at https://theengineroom.org.

Executive Summary

Technology gives us superpowers – but it is also our Achilles heel.

At a time of shrinking civic space across the world[1], digital attacks and digital threats are on the rise. Effective defence and preparation is increasingly critical for a well-functioning civic space, especially for organisations and communities seeking to hold those in power accountable.

Conceptually, digitally securing organisations can be compared to preparing an office against fire, in that there are multiple levels at which preparation is needed:

- **Infrastructure:** buildings are designed with fire protection in mind – from cladding in the walls, to building in accessible fire escapes. Similarly, organisations should be thinking about their organisational security when setting up and maintaining their operational infrastructure.

- **Response levels:** in case of fire, there are multiple options available – from calling the operator in case of a big emergency, to using a fire extinguisher. There are also different triggers that instigate a response – smoke alarms, sprinkler systems, or manually triggering the fire alarm. For organisations, different levels of digital security threats warrant different responses and types of expertise.

- **Culture and knowledge:** responses to fire differ from country to country. Advice to "turn the sprinklers on" in a country where sprinklers are not used, is not helpful – just as digital security advice like "use an iPhone" in a country where Android phones are the norm is not helpful. Building up literacy and developing a culture that prioritises security and safety takes time, and requires repetition and maintenance.

Societies the world over recognise that fire protection at each of these levels is crucial and life-saving. That is not (yet) the case when it comes to digital security: despite our growing dependence on digital technologies, the digital security support ecosystem has not evolved

[1] See, for example: Camila Bustos, "The Shrinking of Civic Spaces: What is Happening and What Can We Do?", Dejusticia, 17 April 2017: https://www.dejusticia.org/en/the-shrinking-of-civic-spaces-what-is-happening-and-what-can-we-do/.

to meet the realities and needs of civil society. The support ecosystem remains dominated by context unaware support providers who often focus on niche technical solutions, ignore long-term infrastructure needs, and fail to properly address the cultural practices that need to be developed. Robust, long-term investment is needed at each of these levels to create an overall healthy ecosystem.

Historically, philanthropy and the digital security ecosystem has focused on the most visible and immediately-rewarding aspects of support: building new tools and applications, and providing short-term technical support. This has left infrastructural pieces that are necessary for strong civil society under-resourced and under-developed, including organisational security. Without secure organisations, civil society will not be able to effectively serve the public interest in the long term.

The digital security support ecosystem is multifaceted, each part supported and watched over by different actors working towards complementary, but different, objectives:

- Physical infrastructure: States, corporations or communities building resilient physical infrastructure to provide access to the internet. (Compare to: building a resilient water access infrastructure so buildings have access to water to put fires out.)

- Technical standards: Technical standards bodies ensure that the way in which the Internet works builds in privacy-protecting measures. (Compare to: developing institutionally-agreed upon quality assurance building standards.)

- Legal frameworks and policy: lawyers and policymakers ensure that legal frameworks and policies respect human rights in the digital sphere. (Compare to: ensuring appropriate legal responses against arsonists are present, or insurance policies against accidental fire.)

- Technical development: Development of software to allow for secure digital practices. (Compare to: developing innovative products that are fire-resistant.)

Civil society organisations intersect with the above elements, and have needs that are unique to their role of holding power accountable and often being the first point of attack. This report focuses on the digital security support ecosystem from the perspective of the civil society organisations, and suggests actions that funders and members of the digital security support ecosystem could take to better meet these organisations' needs.

In 2018, civil society is almost entirely reliant on technology to operate, from information management to basic communication. Our digital infrastructure connects us at a broader scale than ever before, but it opens up new vulnerabilities that often remain invisible until they are used against us. At the same time, many civil society organisations face severe resource constraints forcing them to choose between their mission-driven work and investments in their own security, often to the detriment of both. A large part of correcting this lies with philanthropy: to ensure that incentives are in place to encourage better security practices and to support the digital security support ecosystem at all levels.

Put simply: ignoring digital security undermines the mission of any civil society organisation today.

For civil society organisations to continue operating at scale, we must begin developing healthy practices that address digital security at all levels, from using and developing user-friendly, secure technology tools, to storing data securely, and, above all, developing an organisational culture which integrates and values digital security. For that to happen, we need the digital security support ecosystem to evolve, learn from past mistakes, and meet civil society's needs.

Key points

Context

Digital security is best understood within the context of political and social environments, and within the role it plays in an organisation's fabric and infrastructure. Understanding these four points is key to understanding the recommendations that follow.

- **Security is multi-dimensional:** particularly for civil society organisations working in stressful and risky conditions, safety and security consists of many dimensions: physical, psychosocial, and organisational. For support measures to be successful, they need to be holistic, recognising and addressing security as a complex social, political and technical issue.

- **Digital security is becoming increasingly criminalised:** particularly in politically restrictive countries, taking measures to secure yourself digitally is seen as a political act. Examples include digital security trainers being imprisoned in Turkey; encryption being ruled illegal in Pakistan; and online anonymity being considered unconstitutional in Venezuela.

- **Security is contextual:** advice intended for one organisation might be totally irrelevant, useless, or, at worst, harmful for another. Context changes how technologies are used and implemented by organisations – and as such, affects which security practices are relevant for different communities.

- **Digital security is a series of practices, not a one-off:** healthy digital security practices are ongoing behaviours, which need to be updated as the political and technical environment changes. Mastering digital security means establishing practices in order to learn, evolve and update one's behaviour.

Recommendations

These recommendations are drawn from interviews with digital security support providers, digital security experts, and recipients of digital security support, with a particular focus on the United States. All recommendations are responses to problems raised consistently and repeatedly by interviewees, suggestions directly from multiple interviewees, or drawn from digital security challenges observed over time through The Engine Room's own experience as a support organisation for civil society.

Strengthening the digital security support ecosystem

The following recommendations cover supporting the digital security support ecosystem as a whole.

- **Fund analysis of digital attacks experienced by civil society organisations:** Systematic research on attacks experienced by civil society globally could reveal patterns in types of attacks, and increase the community's ability to accurately respond to these threats.

For example: looking into spyware sent over email to civil society groups on a systematic, global scale.

- **Support targeted advocacy towards leadership of organisations about the importance and relevance of digital security for their organisation:** interviewees highlighted a generational gap in attitudes towards digital security, as well as a lack of accessible digital security advocacy materials targeted at older members of civil society, who often hold leadership positions that oversee budgets and priorities. Understanding digital security is particularly important for leadership who sit at these positions of decision-making, and who might be new to some of these issues. For civil society organisations to prioritise digital security, advocacy needs to happen at all levels of organisational structure and hierarchy.

- **Support the development of accessible, community-relevant materials addressing digital security:** these should be developed by organisations or communities who are themselves members of the target users. This would allow the resource creators to realistically identify both the need for materials as well as the existing capacity, and ensure they are able to share these resources for use with organisations within their existing networks.

- **Support community management for networks of digital security support providers:** although networks of technical digital security support providers are growing, they risk not reaching their potential target audience and not documenting their learnings in a way that contributes to shared knowledge. This could be mitigated by encouraging networks of technical providers to invest in community management. People tasked with community management would play an operational/support role to the network, focusing on developing documentation, building streamlined processes for support provision and sharing learnings with other relevant communities.

- **Prioritise requests for security support** from staff, grantees, volunteers alike. Model healthy behaviour of taking security seriously to demonstrate that security is a priority for an organisation. Where possible to do so responsibly, share that this has become a priority (eg. to an organisation's board; through a public statement; in a staff meeting).

- **Encourage people from under-represented communities to engage with digital security support provision**. Currently, there is a big capacity gap, with a serious lack of people from affected communities who both understand context and digital security issues, and have existing strong relationships within those communities. In the long-term, addressing this capacity gap is an essential piece of a healthy digital security support ecosystem.

- **Build networks between "accidental techies" in grantee organisations:** these are the people who, often without a formal technical background, end up being responsible for organisational security. This role can be challenging and stressful, and often they end up operating alone. Make connections between accidental techies in grantee organisations to provide them with peer support and inspiration.

For philanthropy

- **Reward organisations who make great strides in their organisational security,** by increasing their core funding over time. This sends a message to other organisations that prioritising organisational security is an important part of organisational growth, and contributes to the longer-term capacity building of more people with organisational security skills who are rooted within movement work.

· **Reduce support for generalised guides and generalised resource websites.** We heard multiple times that “all-purpose” resources are not meeting the needs of any particular group, with many finding them not specific enough for their context. Instead, identify key communities and groups in need of resources, and institutions best placed to understand their needs and design resources accordingly.

· **Support projects that interlink investigation into attacks on civil society, strategic litigation, technical development, and user-centred support.** Digital security is not a standalone support mechanism, and needs to be linked with other key institutional foundations to be successful.

· **Consider organisational security as part of operational support:** For some, organisational security fits within the operations team of the organisation – from ensuring that emails are hosted securely, to running finance software and budgeting. But interviewees suggested that finding core support which includes budget for organisational security is much harder to find than project-based funding.