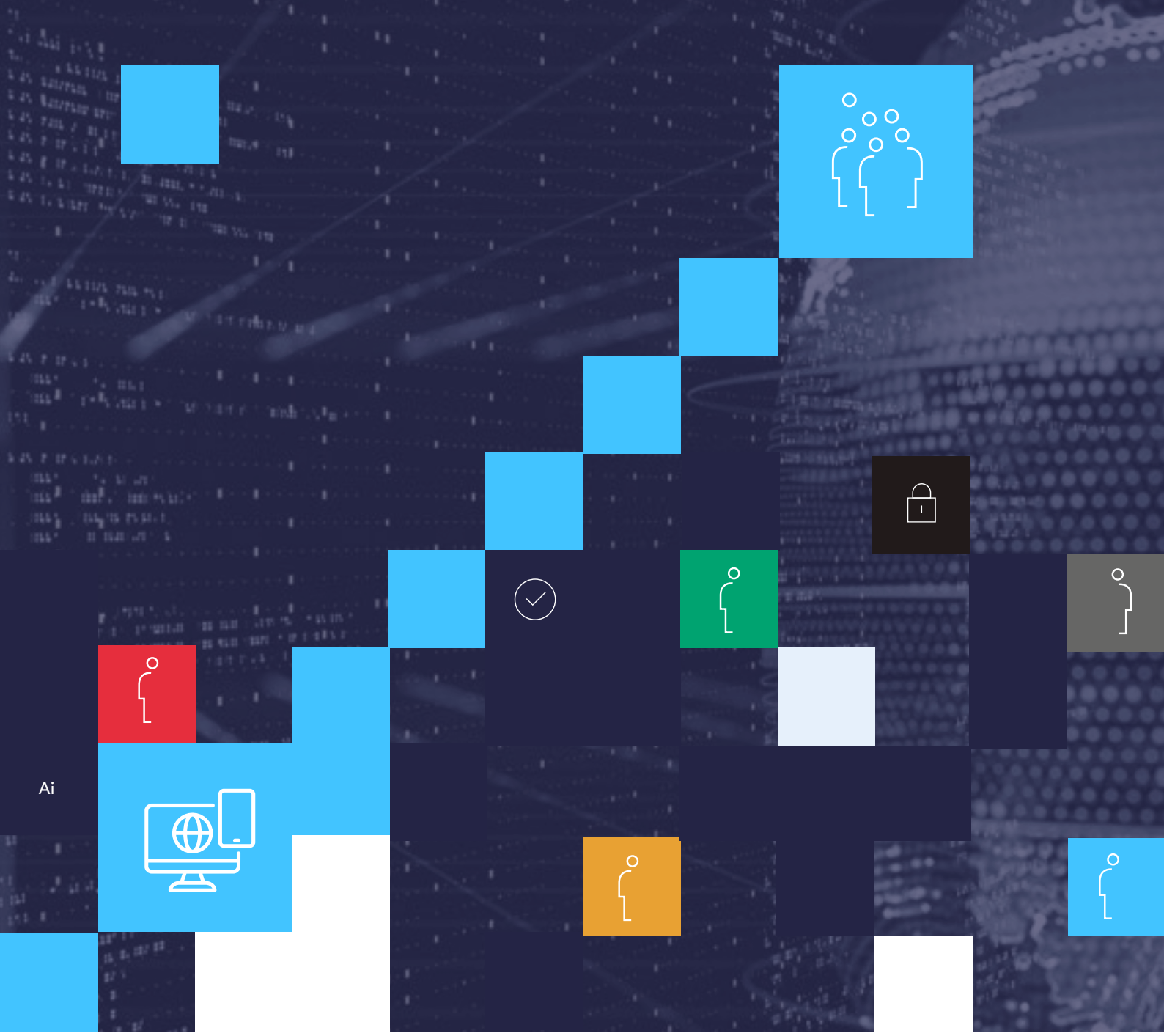


FROM PLATFORMS TO COMMONS:

A Field Guide to Participatory, Decentralised and Community-Owned Infrastructure

2025

Prepared by Human Future Agency for the Civicus Coalition Hub

CIVICUS

human future. agency

Foreword

Civil society is working through a period of growing digital uncertainty. Organisations rely on systems and platforms that are shifting quickly, often in ways that limit civic space, increase operational risk and reduce the ability of communities to organise safely. Funding pressures, political constraints and uneven digital capacity make this harder across many regions.

At the same time, new approaches are emerging. Across different movements and contexts, practitioners are testing models that give communities greater control over data, decision-making and digital infrastructure. Experiments with public-interest technology, shared governance and decentralised systems are still in the early stages, but they offer useful signals about what more resilient civic infrastructure could look like.

This report, prepared for the CIVICUS Coalition Hub, brings together a curated set of these developments. It draws on global discussions at International Civil Society Week, MozFest, Web Summit and recent digital sovereignty gatherings, alongside conversations with technologists, organisers and researchers. It is not a complete map of the field, but an attempt to surface promising ideas, relevant risks and practical entry points for CIVICUS and civil society actors exploring this space.

The aim is straightforward: to help leaders, organisers and partners build a clearer view of the landscape and identify where experimentation may strengthen people-powered action. No single organisation can do this alone, but shared understanding and collaborative effort can put civil society in a stronger position to shape the next generation of digital infrastructure.

Contents

Part I.
Context and Purpose

Civil Society in 2025: A Changing, Constrained and Fragmented Landscape

Civil society in 2025 operates in an environment shaped by political turbulence, economic uncertainty and rapid technological change. The pressure on civic actors has intensified, yet the scale and form of these pressures differ significantly by region. What is consistent, however, is the growing interdependence between civil society and digital infrastructure. Activists, advocates, service providers and social movements now rely heavily on platforms and technologies that they do not control. This reliance exposes them to new forms of vulnerability at the very moment when public leadership from civil society is most needed.

This section highlights several insights and findings from the CIVICUS Monitor, the World Economic Forum, Access Now, Freedom House, the OECD and regional digital rights organisations. The goal here is not to produce a comprehensive analysis, but to outline the key conditions that shape why alternative, participatory and community owned digital infrastructures matter.

Many of the themes below consistently surfaced across sessions and breakout discussions at International Civil Society Week, MozFest, Web Summit and recent digital sovereignty gatherings in Berlin and France.

1.1 Shrinking civic space

According to the CIVICUS Monitor 2024 to 2025 update, only 3 percent of the global population live in countries classified as open civic space. More than 80 percent live in contexts that are considered obstructed, repressed or completely closed.
Source: https://monitor.civicus.org

Across every region, there has been an increase in:

- restrictions on protests and assemblies
- excessive use of force or criminalisation
- arbitrary content moderation orders
- legal actions against media and activists
- digital surveillance of human rights defenders

Freedom House's 2025 Freedom on the Net report found that internet freedom declined in 26 countries and improved in only 9, continuing a 14 year downward trend.

- **Source:** https://freedomhouse.org/report/freedom-net

These patterns indicate that civic freedoms are increasingly shaped by digital conditions. When online spaces are restricted or manipulated, offline civic space narrows as well.

1.2 Reliance on a fragile digital infrastructure

Most civil society organisations operate through commercial platforms and cloud services whose governance, algorithms and business models are outside their influence. The transition to remote working and digital organising during the pandemic deepened this dependency.

Several recent studies point to increasing operational vulnerability:

- Researchers from Oxford Internet Institute and Carnegie Endowment (2024-2025) note that the **concentration of key internet services in a handful of companies raises systemic risk** for public interest work.
  - **Source:** https://carnegieendowment.org

- **Algorithmic changes made by major platforms in 2024 without public notice led to sudden drops in reach for many civic groups,** particularly in the Global South, as documented by Global Voices and SMEX.
  - **Sources:** https://globalvoices.org and https://smex.org

This fragility is structural. Civil society's digital backbone currently depends on infrastructures that prioritise profit, scale and data extraction. These incentives often run counter to the needs of movements, communities or human rights defenders.

1.3 Information disorder, Gen AI media and eroding trust

Generative AI has transformed the information environment. According to the World Economic Forum Global Risks Report 2025, misinformation and disinformation are ranked as a significant global risk over the next two year horizon.
- **Source:** https://reports.weforum.org

New patterns include:
- realistic audio and video impersonations
- targeted influence campaigns during elections
- fabricated civil society statements or forged evidence
- confusion over authentic organisational communication
- amplified harassment and coordinated online attacks

In 2024 and early 2025, more than 40 national elections saw serious incidents of deepfake based misinformation, according to research by the Brookings Institution and the European Digital Media Observatory.
- **Sources:** https://www.brookings.edu and https://edmo.eu

Civil society organisations face a dual challenge. They must defend communities against manipulation while navigating the same polluted information systems to advocate and coordinate their own work.

1.4 Climate related and geopolitical disruptions to infrastructure

Climate change increasingly affects digital systems. Floods, extreme heat, wildfires and storms are impacting data centres, undersea cables and power grids. The UN Office for Disaster Risk Reduction and ITU highlight that climate related outages are rising in frequency and are projected to increase further between 2025 and 2030.

- **Sources:** https://www.undrr.org and https://www.itu.int

In parallel, geopolitical tension has led to:

- targeted throttling or shutdowns of the internet
- cross border data access restrictions
- cyber attacks on civil society organisations and human rights networks
- the emergence of parallel digital ecosystems shaped by national security priorities
- Information warfare at scale

Access Now documented 283 internet shutdowns in 2023 and notes that 2024 and early 2025 continue this trend, with shutdowns linked to elections, protests and emergencies.

- **Source:** https://www.accessnow.org

These disruptions disproportionately affect activists and organisations that rely on digital tools for coordination and safety.

1.5 Regulatory fragmentation and the rise of competing digital spheres

A growing number of governments and regional blocs are developing autonomous digital strategies, including national cloud systems, sovereign AI frameworks and data localisation rules. This has resulted in an increasingly fragmented digital landscape.

Examples include:

- The European Union's Data Governance Act and AI Act
- India's Digital Public Infrastructure strategy
- Brazil's emerging sovereign AI agenda
- China's strict data localisation rules
- African Union work on cross border data governance (2024 to 2025)

Although there are several aspects to these frameworks that are welcome, this fragmentation creates operational uncertainty for NGOs. Cross border collaboration becomes more complex, compliance burdens increase and organisations face divergent standards around privacy, data storage and AI transparency.

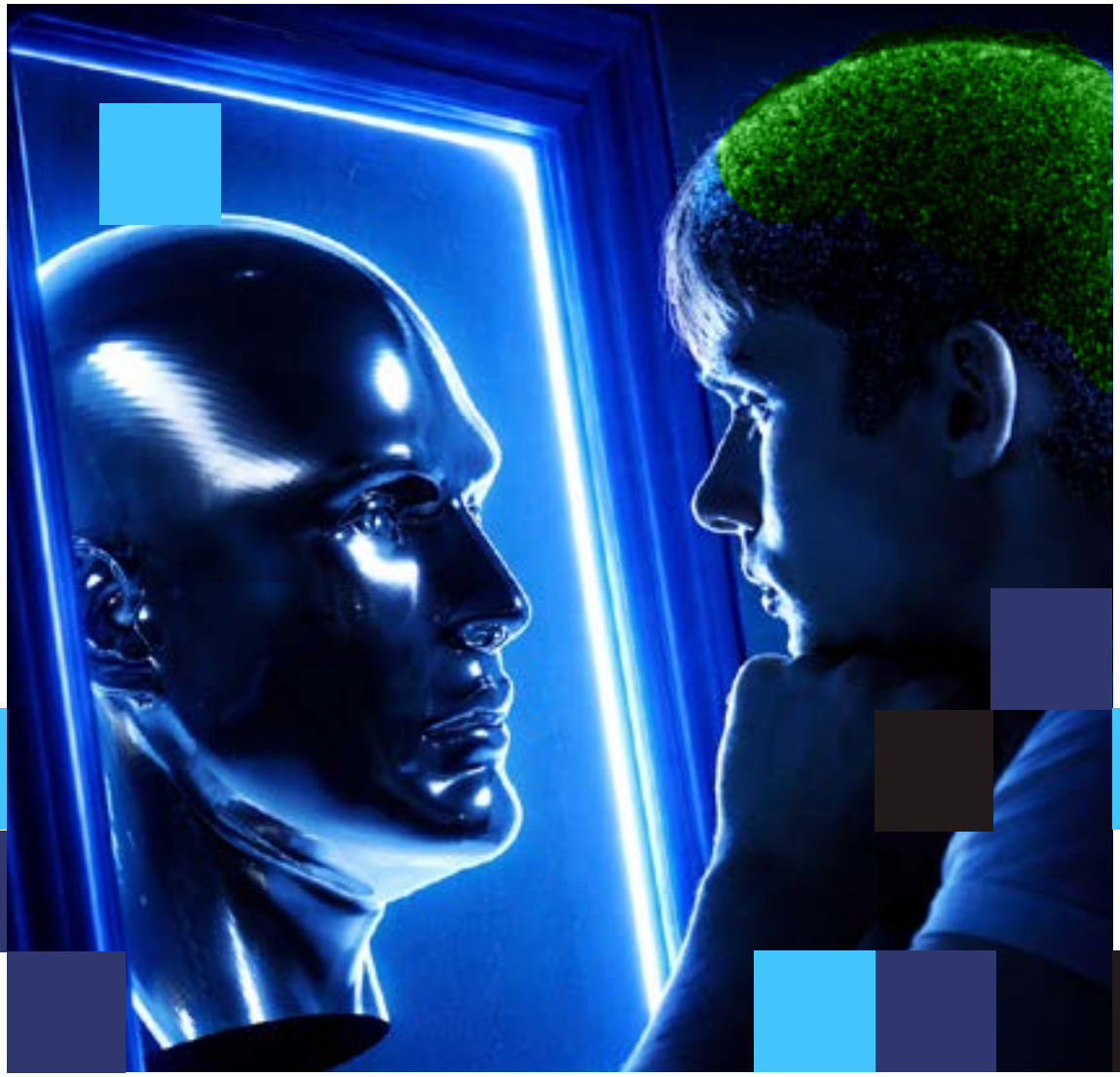
Why this context matters

Civil society in 2025 needs to think not only about political pressures, systems and the effects of economic disparity but also about the structural fragility of the digital foundations it relies on to communicate to the world.

The combination of platform dependence, information disorder, climate risk and geopolitical fragmentation creates a strategic challenge. Traditional tools and assumptions are no longer sufficient.

This report therefore explores whether participatory, decentralised and community owned technologies could help civil society strengthen resilience, autonomy and collective power in a rapidly changing world.

The following sections build the conceptual foundation for that exploration.



Part II.
Core Concepts

2.1 Participation and Co-Governance

Civil society has spent decades improving methods for consultation, organising, representation and collective decision making. What has changed in recent years is that many of the spaces where this work now takes place are digital and controlled by actors outside the public interest. This shift raises a fundamental question that came up repeatedly in consultations across International Civil Society Week, MozFest, Web Summit and digital sovereignty forums.

How can civil society maintain meaningful influence when the infrastructure it depends on is governed elsewhere?

Participation in digital environments is often shallow. People can post, comment or react, but they have little influence over how systems operate, what data they collect, how algorithms behave or how content is moderated. Even digital tools marketed as participatory sometimes replicate the same centralised governance structures that civil society has been pushing back against for decades.

Co-governance offers a way to respond to this challenge. It focuses on how decisions are made, who gets to shape the rules, and how communities can exercise real authority over the systems they rely on.

What participation means in digital systems

In the context of digital infrastructure, participation is not simply about speaking or being heard. It is about:

- the ability to influence how decisions are made
- the transparency of rules and operations
- the capacity to challenge harmful outcomes
- having reliable ways to hold system operators accountable
- the presence of inclusive, community anchored processes

When civil society uses digital tools without the ability to influence these elements, participation becomes fragile and easily undermined.

Why co-governance is essential for decentralised and community owned tech

Most decentralised technologies claim to offer more autonomy to users, but without clear governance models they risk becoming:

- technically decentralised but decision making centralised
- open source but controlled by small elite groups
- participatory in appearance but unequal in practice

Co-governance provides the missing layer. It ensures that communities, particularly those affected by digital harms, have real influence over:

- rules about data use
- moderation and safety policies
- resource allocation
- development priorities
- oversight mechanisms
- crisis response protocols

Without co-governance, decentralised infrastructure becomes just another technical experiment that does not shift power.

Examples of co-governance relevant to civil society

Several models surfaced across consultations and research. They are not perfectly adapted for the digital world, but they illustrate how shared authority can work in practice.

Community rule setting: Users collectively shape the policies that govern a platform.
For example, participatory policy making in Decidim and Taiwan's vTaiwan process.

Shared oversight: Independent community bodies monitor decisions and publicly document changes.
For example, community driven moderation panels in federated social networks.

Participatory resource planning: Communities have a role in setting priorities or allocating budgets, particularly for digital public goods or open source projects.

Multistakeholder working groups: Civil society, technologists, governments and affected communities work together on governance of specific tools or standards.

Challenges and questions to take seriously

Consultations highlighted several open questions that civil society leaders must confront when designing governance systems for participatory technology:

- How to prevent co-governance processes from being dominated by well resourced actors?
- How to include groups who face access, language or disability barriers?
- How to balance expertise, representation and equity?
- How to sustain participation when resources are limited?
- What decisions should remain centralised for safety or legal reasons?
- How to resolve conflict in shared governance spaces?

2.2 Identity, Trust and Human Verification

Digital identity has become unstable in ways that directly affect how civil society operates. Technologies that once felt peripheral now shape whether people can organise safely, participate meaningfully or trust the information in front of them. The growing availability of generative AI has made impersonation, falsified audio and fabricated statements more common and more convincing. Research from the European Digital Media Observatory and the Stanford Internet Observatory in 2024 and 2025 shows an increase in synthetic accounts and deepfakes aimed at discrediting public interest organisations. The World Economic Forum's Global Risks Report 2025 identifies misinformation and synthetic content as the highest short-term threat to global stability.

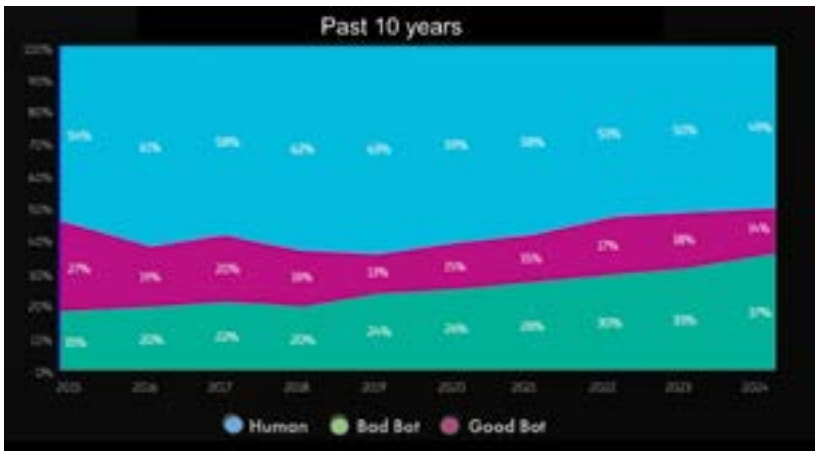
- **Sources:** https://edmo.eu and https://cyber.fsi.stanford.edu and https://reports.weforum.org

Civil society often experiences these shifts first. Activists face targeted impersonation. Organisations receive fabricated messages that appear to be from partners. Public audiences struggle to distinguish genuine communication from manipulated media. These dynamics create an operational challenge that affects everything from campaigning to community engagement.

Why identity is becoming harder to rely on

Digital identity has entered a period of instability. For many years, people relied on simple cues to judge authenticity online. A familiar username, a writing style, a profile with a history of posts or a video that appeared genuine were usually enough to trust that an interaction involved a real person. These cues no longer provide reliable assurance.
A major reason is the rapid spread of generative AI. Tools that imitate voices, faces and writing styles now operate at a level that makes manual detection extremely difficult. A short audio sample can be cloned. Video footage can be convincingly altered. Written communication can be generated to match a person's tone or the norms of a local community.

At the same time, automated systems that imitate human behaviour have become far more sophisticated. These include traditional bots, as well as newer hybrid systems where human oversight and automated generation blend together. They can maintain plausible posting patterns, mimic community language and react in real time, which undermines the assumption that a persistent online account must represent a real individual.



Composition of internet traffic (past 10 years). The rise in the number of accessible AI tools has significantly lowered the barrier for entry for cyber attackers enabling them to create and deploy malicious bots at scale. Bad Bot Report 2025

Authentication systems have not kept up with these developments. Password based systems are insecure, SMS verification can be intercepted, commercial verification labels can be purchased, and biometric identity remains highly contested due to privacy risks and the consequences of any data breach.

Finally, identity standards are diverging across regions. The European Union is moving toward digital wallets, some governments continue to expand biometric schemes and others rely on device level or behavioural identifiers. These approaches are often incompatible and follow different legal and political logics, which adds further uncertainty. The result is a landscape where identity is easy to imitate and increasingly difficult to confirm. Civil society has to operate within this broader shift, recognising that many older assumptions about authenticity and trust are no longer reliable.

The difference between identity and verification

Identity and verification are frequently treated as synonyms, but they serve different purposes. Identity is about who someone is. Verification is about confirming that an interaction involves a real human acting in good faith.

Most civil society activity does not require formal identity. It requires confidence that:

- a participant is not an automated agent
- a message originates from a legitimate source
- people in a shared process are who they claim to be in context
- participation is safe even when anonymity is necessary

In practice, this means distinguishing between three related concepts that are often blurred together. **Authentication** refers to proving that a person controls a specific account or credential, for example logging in with a password, passkey or secure token. Identification describes linking that account or credential to a known individual, which is only needed in limited circumstances such as safeguarding or legal compliance. Verification is the middle layer. It confirms that a real, accountable human is participating without requiring them to reveal their personal identity. Many civic processes only require verification. Participants can remain pseudonymous or anonymous while still giving others confidence that they are genuine, unique and participating with integrity.

This distinction matters because systems that require formal identity, such as biometric databases or centralised national ID frameworks, often introduce risks that are unnecessary for most civic processes. When identity is tied to state-issued documents or sensitive personal data, participants can be exposed to surveillance, profiling or data misuse. These systems can also exclude people who lack official documentation, who face discrimination when accessing ID services or who rely on anonymity for their safety. Research from Privacy International (https://privacyinternational.org) and Access Now (https://www.accessnow.org) shows that these harms are especially acute in environments with weak safeguards, limited oversight or politicised use of digital infrastructure. For this reason, civil society requires verification models that are proportionate, privacy preserving and appropriate to the local context. The goal is to confirm that a real human is taking part, not to force individuals to surrender their identity in situations where it is neither necessary nor safe.

Approaches to verification that are emerging

As older cues of authenticity disappear, new ways of confirming that a real human is taking part in a digital interaction have begun to emerge. These approaches differ in method and maturity, but they reflect the same underlying reality. Identity can no longer be assumed, so verification has become part of the infrastructure of trust. One approach relies on social trust built over time. In long standing communities such as Debian or Wikimedia, a person becomes credible because others have observed their behaviour and contribution across many interactions.

This makes impersonation harder. The drawback is that this only works in communities where people already have a shared history. It is not a practical solution for large public processes with many newcomers.

Another direction focuses on what is often called proof of personhood. The aim is to confirm that someone is a real, unique human without requiring them to reveal their identity. Different projects take very different routes. BrightID uses a network of people vouching for one another. Proof of Humanity uses short video submissions that others can challenge. The heavily criticised Worldcoin project uses iris scans to generate a unique biometric code. These examples sit under the same broad idea but raise very different questions about privacy, power and control. Some approaches lean on social networks. Others rely on sensitive data. The underlying concept is promising, but the implementations vary in their risks and values.

A third set of methods uses technical signals from devices. Technologies such as WebAuthn and platform attestation systems can distinguish actions performed by a real device from basic automated activity. These tools can reduce simple manipulation but depend heavily on large technology companies and do not resolve questions about who controls the verification layer or how to protect vulnerable participants.

None of these approaches is sufficient on its own. Verification is moving toward a blend of social recognition, technical proof and contextual judgement. Civil society will need to understand how these methods work, not necessarily to build them, but to recognise which systems support privacy, safety and fair participation, and which recreate the very power imbalances they are meant to address.

Risks and ethical considerations

Verification systems can cause harm if they are designed without regard for safety, inclusion or political context. Some approaches require hardware, connectivity or documentation that many people do not have.

Others create centralised databases that could be accessed by hostile authorities. Even privacy preserving systems can create a false sense of security if they are not well understood.

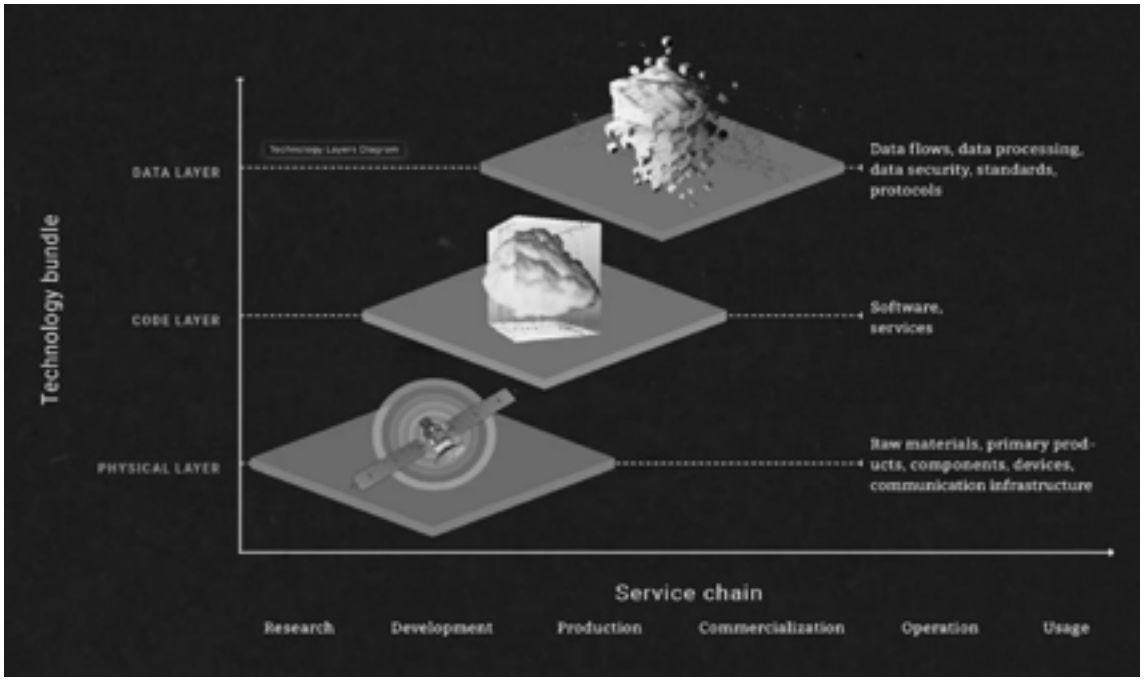
Another challenge concerns governance. Verification systems grant significant power to whoever controls them. Decisions about who is allowed into a process, who appears legitimate or whose participation is restricted carry political weight. These decisions can shape who feels safe to speak and who is excluded.

Civil society needs verification approaches that reinforce rather than undermine its values. This includes transparency about how verification is carried out, clear lines of accountability, protections against misuse and methods that avoid reinforcing social inequalities.

2.3 Digital Commons, Sovereignty and Civic Autonomy

Digital infrastructure is made up of several interdependent layers:

- **raw materials and hardware** (chips, fibre, devices, data centres),
- **code and standards** (protocols, APIs, algorithms),
- **data and models** (training corpora, identity systems, content ranking), and
- **services** (platforms, hosting, authentication and communication tools).



Sovereignty debates in 2025 centre on who controls these layers and under what terms. Research from Open Future (2025), the OECD (2024) and the EU Sovereign Tech Fund shows that many essential components (e.g. cloud environments, identity services, payment rails and large-scale AI infrastructure) are governed by a small number of companies and jurisdictions. Because these layers determine how information moves, how identities are verified and how participation happens, external control introduces operational and political uncertainty.

Regional responses reflect different priorities:

- **Europe** focuses on rights-based regulation and publicly governed digital services.
- **Asia (selected regions)** embeds key systems firmly within state-led infrastructure strategies.
- **Africa (selected regions)** prioritises reducing foreign dependency and improving service continuity in environments shaped by shutdowns, bandwidth constraints and limited local hosting. These patterns are documented by SMEX, CIPESA, Derechos Digitales and GovStack deployments.

For civil society organisations, these issues show up as reliability problems rather than policy debates. Analyses from EDMO, the Stanford Internet Observatory and Freedom House highlight how platform rule changes, service removals or outages can interrupt communication, delay coordination and destabilise public-facing work.

In response, attention is shifting toward **digital commons** - shared digital resources governed transparently and in the public interest. Commons-based approaches operate at different layers:

- At the **code and standards layer**, projects such as ActivityPub and ATProto enable interoperability so that communities are not locked into single providers.

- At the **application and service layer**, platforms like Decidim and Open Collective use governance structures where development, resourcing and policy decisions are participatory and accountable.

- At the **infrastructure layer**, early initiatives such as **Eurosky (also see 3.1)** are exploring whether hosting, content curation and moderation frameworks can be operated by public-interest institutions. Eurosky is testing whether federated social systems can remain interoperable with global networks while aligning ranking, moderation and safety logic with democratic oversight rather than commercial priorities.

These initiatives are not full solutions to political pressure or information manipulation, and they do not eliminate risk. Their practical value lies in increasing the number of credible alternatives available to organisations. When infrastructure conditions change—whether due to platform policy shifts, outages or regulatory interventions—-commons-based and sovereign-aligned systems provide additional routes for communication, participation and coordination.

In a digital environment that is becoming more fragmented and less predictable, diversification across data, code and infrastructure layers supports continuity, resilience and operational autonomy for civic actors.

Part III.
Global Landscape Mapping

The concepts outlined in the previous sections are already influencing how new digital systems are being built. Around the world, a wide range of actors are experimenting with infrastructures that distribute control, strengthen public oversight or reduce dependency on large commercial platforms. These projects differ in purpose and maturity, but together they show how the digital landscape is beginning to shift.

Part III focuses on the most relevant types of emerging infrastructure. It highlights representative examples, explains the basic logic behind each mechanism and outlines why these models matter for civil society.

3.1 Public Interest Social Infrastructure

Public-interest social infrastructure refers to digital spaces that function like social platforms or communication systems but are designed around public benefit rather than commercial profit. These systems run on open technical standards, can be hosted by many organisations and allow their rules and moderation processes to be shaped in more transparent and accountable ways. The aim is to reduce dependency on commercial platforms and to create environments that reflect public values rather than advertising or shareholder incentives.

Interest in this model has grown as large commercial platforms have become more fragile and unpredictable. Sudden policy shifts, changes in ownership, opaque recommendation systems and inconsistent moderation practices have created clear risks for civil society groups that depend on them for communication. In response, a number of public-oriented initiatives have emerged that illustrate alternative approaches to digital infrastructure.

One of the most significant recent efforts is **Eurosky** (placeholder URL: https://eurosky.eu), a European initiative that aims to develop a publicly governed social network built on open protocols rather than a single commercial platform. Eurosky is linked to broader European goals around digital sovereignty, which refers to the ability for governments, institutions and citizens to rely on infrastructure that they can understand, influence and, where necessary, control. Early Commission papers and OECD reports point out that Europe still depends heavily on non-European companies for cloud hosting, digital identity systems, AI models and the raw materials and chips that power hardware. Eurosky is intended as one component of a more accountable ecosystem. It proposes a shared social networking layer that public bodies, civil society organisations and approved independent hosts can operate. It also explores links with emerging European digital identity frameworks, data portability standards and governance structures designed to avoid both corporate and state capture.

Alongside Eurosky, the **Fediverse** has become a practical demonstration of decentralised social infrastructure. It is built around the **ActivityPub protocol** (https://www.w3.org/TR/activitypub), which allows different services to communicate with each other. Platforms such as **Mastodon** (https://mastodon.social) and **PeerTube** (https://joinpeertube.org) show how thousands of independently hosted servers can form a single network without any central owner. Each server can set its own moderation rules and community guidelines, and users can still interact across servers because they share the same protocol. This creates a more resilient and community governed environment for social communication.

Cities have also experimented with public-interest digital tools. Barcelona's long running platform **Decidim** (https://decidim.org) provides an open source system for public

participation. Residents can make proposals, take part in consultations and follow decision-making processes in a transparent way. Decidim is jointly governed by the municipality, civic organisations and independent contributors. Although it is not a social network, it shows how public institutions can steward digital platforms in ways that give communities meaningful influence.

There are also ecosystem support organisations that maintain and host open tools. **Framasoft** (https://framasoft.org) in France provides hosting, training resources and free alternatives to commercial software. In India, the India Stack digital public infrastructure programme (https://www.indiastack.org) provides open identity, payments and data exchange systems that can be used by both the public sector and independent developers. These initiatives differ in purpose and governance models, but they reflect a shared approach that prioritises transparency, interoperability and long-term public value.

Taken together, these projects point toward a distinct model of digital environment. Public-interest social infrastructure is built on open standards, shared governance and distributed hosting rather than concentrated corporate control. The specific implementations vary, but the direction is consistent. The aim is to create digital spaces where power, influence and accountability can be shared rather than captured.

3.2. Community Data and Open Source AI Ecosystems

As AI systems become central to communication, translation and information access, the question of who builds them and whose data they reflect has become increasingly important. Community data and open source AI ecosystems are emerging as an alternative to large commercial or state-controlled models. These efforts aim to ensure that languages, cultures and communities that are usually underrepresented in mainstream datasets have a direct role in shaping the systems that will affect them.

One of the strongest examples is Masakhane, a pan African grassroots research community working on natural language processing for African languages. Its work is entirely open, community driven and based on the idea that people who speak a language should guide how it is represented in AI systems. Masakhane has produced datasets, translation models and research that would not exist otherwise.
Link: https://www.masakhane.io

In Latin America, initiatives such as LatinX NLP (https://latinxnlp.org) and regional open data collectives have taken similar approaches, creating corpora and models that reflect the linguistic diversity of the region. These projects operate with strong volunteer energy and are filling gaps left by commercial AI models that largely prioritise English and a small set of global languages.

Several countries are exploring more structured approaches. Brazil has begun investing in sovereign AI models developed with public research institutions, aiming to ensure that national datasets and public sector use cases are not entirely dependent on foreign providers. Kenya, Rwanda and the GovStack community (https://www.govstack.global) are developing open, modular digital infrastructure components that can support public services, including AI-enabled systems, with shared governance and local oversight.

The open source AI ecosystem has also expanded rapidly. Projects like Hugging Face (https://huggingface.co) have become central hubs where models, datasets and evaluation tools are shared openly. Although not all models are community governed, the ecosystem allows civil society groups, researchers and local institutions to experiment, audit and adapt AI systems without relying exclusively on proprietary services.

These examples show a mechanism where data and model building are shaped by the communities that need them, rather than extracted from them. Community data ecosystems do not solve all the challenges of AI, and they often lack stable funding, but they offer a path toward systems that reflect linguistic diversity, regional realities and public interest needs. This is especially relevant for civil society groups working in contexts where dominant AI models fail or where local languages and knowledge systems are poorly represented.

3.3 Governance and Resource Sharing Infrastructures

Some emerging systems focus less on communication or AI, and more on how groups make decisions, share resources and coordinate work across distance. These infrastructures create structured ways for people and organisations to govern projects together, allocate funds, set rules or track commitments without relying on a single central authority.

A well-known example is the family of tools often labelled as “DAOs”, or decentralised autonomous organisations. The term is messy, but the underlying idea is straightforward. A DAO is a digital structure that lets a group make decisions collectively, record those decisions transparently and manage shared resources according to agreed rules. Many early DAO projects were dominated by speculation, but others have developed more practical governance functions. The **Giveth** community, for example, supports donation and grantmaking processes through shared decision making and transparent funding flows.
Link: https://giveth.io

A different model can be seen in **Open Collective**, a platform that allows groups without legal status to manage shared funds through a fiscal host. Contributions, expenditures and balances are public, and the structure is designed for community projects, local groups and open source initiatives that need transparent resource management without building their own administrative systems.
Link: https://opencollective.com

Some public institutions are experimenting with formalised shared governance. The City of Barcelona’s governance model for **Decidim** includes community representatives, researchers, developers and municipal staff who help guide the project’s evolution. This is not a DAO, but it is a practical example of multi stakeholder digital governance that distributes authority rather than centralising it.
Link: https://decidim.org

There are also sector specific infrastructures. **Hypha Worker Cooperative** in Canada has built shared governance and resource tools for cooperatives and community organisations.
Link: https://hypha.coop

The Aragon project provides modular governance components used by some civil society groups to run structured votes or manage permissions.
Link: https://aragon.org

These systems vary widely, but they all support one function: they allow groups to coordinate decisions and resources in transparent, accountable ways that do not depend on a single gatekeeper. For civil society, this matters because it can reduce administrative overheads, make collaboration more resilient and distribute governance authority across the communities involved.

3.4 Crisis Ready and Offline Infrastructure

Civic work often depends on digital systems that fail precisely when they are needed most. Crises such as natural disasters, conflict, political unrest or targeted shutdowns can cut organisations off from communities and partners. Crisis ready and offline infrastructure refers to tools and networks designed to function when mainstream services are disrupted, unreliable or intentionally blocked.

One strand of this work focuses on **mesh networks**, which allow devices to connect directly to one another without relying on central infrastructure. Projects like **NYC Mesh** in the United States (https://www.nycmesh.net) and **Althea** in the United States and Africa (https://althea.net) show how communities can build distributed communication networks that stay online even when commercial networks fail. These systems are not full replacements for the internet, but they can keep essential communication flowing during outages.

In humanitarian and conflict settings, organisations increasingly turn to **GoTenna** style low bandwidth, off grid systems (https://gotenna.com) or community built LoRa based networks for local messaging. These tools support coordination when mobile data networks are overloaded or deliberately disrupted.

Monitoring also matters. Tools like **OONI** (Open Observatory of Network Interference, https://ooni.org) provide independent measurement of internet shutdowns and censorship events. OONI has become a reference point for civil society groups that need verifiable evidence of network interference.

Some countries have also relied on localised, high resilience hosting for critical civic resources. During earthquakes in Nepal and Türkiye, several NGOs used decentralised storage systems such as **IPFS** (https://ipfs.tech) to distribute emergency information across multiple nodes, reducing the risk of a single point of failure.

There is also a growing field of offline first tools. Applications like **Briar** (https://briarproject.org) allow messaging through Bluetooth or Wi Fi without internet access. **Bridgefy** offered similar functionality during large protests, although security researchers have since raised concerns about its encryption. These examples show how fragile mainstream messaging can be when states intervene in connectivity.

Crisis ready and offline infrastructure is still fragmented and unevenly adopted, but the underlying point is simple. When digital systems fail, civil society needs fallback options. Even basic redundancy can be the difference between maintaining contact and losing it entirely.

3.5 Movement Safety and Collective Security

Civil society groups, especially those working in hostile environments, face increasing levels of digital harassment, surveillance and coordinated attacks. Movement safety and collective security refers to infrastructure and tooling that helps organisations protect themselves, share threat information and respond to incidents together rather than in isolation.

One important area is shared threat reporting. Platforms like **Umbrella** (from Security First, https://securityfirst.org) provide practical, scenario-based guidance for frontline defenders. Regional groups, such as **SMEX** in Lebanon (https://smex.org), maintain incident trackers and rapid response networks that help local organisations document attacks, phishing campaigns and account takeovers.

There is also a growing use of secure communication systems that allow organisations to coordinate without relying on mainstream messaging platforms. The **Cwtch** project (https://cwtch.im) operates peer to peer encrypted group communication that does not require central servers. Some movements use **Matrix** with independently hosted servers to reduce risks associated with commercial providers.
Link: https://matrix.org

Tools for anti doxxing and identity protection are also evolving. **Scrutineer** and **Redact** help people remove exposed personal information from the open web.
Links: https://scrutineer.dev and https://redact.dev

Projects like **Block Party** (https://www.blockpartyapp.com) provide filtering and safety controls for social media harassment, although availability varies by region.

There is also work happening in shared security coordination. Groups within the Internet Freedom Festival community, the Access Now Helpline (https://www.accessnow.org/help) and regional digital rights networks in East Africa and Latin America have built rapid support channels for emergencies such as hacked accounts, device seizure or targeted malware. These networks operate as informal infrastructure, but they are critical when conventional support channels are inadequate.

Movement safety infrastructure remains uneven and under resourced, yet it addresses a fundamental need. Civil society cannot rely on commercial platforms to provide adequate protection, and many of the threats organisations face are coordinated across borders. Shared tools and networks give groups a way to respond collectively, distribute the burden of defence and avoid becoming isolated targets.

3.6 Regional Snapshots

The regional landscape shows that the conditions shaping digital infrastructure are far from uniform. Some regions have strong community networks or established digital rights movements, while others operate under severe constraints, including shutdowns, surveillance or fragile connectivity. Despite these differences, a common pattern is emerging. Across continents, civic actors are building or adapting tools that give them more control over communication, data and governance. The initiatives listed in the table illustrate how these efforts are taking shape in very different environments, and why any global strategy needs to account for this diversity rather than assume a single model will work everywhere.

Region	Key Characteristics	Notable Initiatives (with links)	Main Challenges	Opportunities
Africa	Strong community led tech, improving connectivity, frequent shutdowns	Masakhane (https://www.masakhane.io), Zenzeleni (https://zenzeleni.net), Mesh Bukavu, GovStack adoption (https://www.govstack.global)	Shutdowns, limited local hosting, reliance on foreign platforms	Community data ecosystems, public interest connectivity, language AI
Latin America	Long tradition of digital rights organising, strong open data culture	Derechos Digitales (https://www.derechosdigitales.org), LatinX NLP (https://latinxnlp.org), Decidim deployments	Misinformation, political polarisation, uneven infrastructure	Community governed participation tech, localised AI resources
Middle East and North Africa	Highly uneven infrastructure, strong digital rights hubs despite repression	SMEX (https://smex.org), 7amleh (https://7amleh.org), independent tech collectives	Surveillance, platform bias, shutdowns	Resilient hosting, shared threat reporting, decentralised alternatives
South Asia	Large digital populations, identity linked service systems, strong activist networks	IndiaStack (https://www.indiastack.org), Digital Rights Foundation (https://digitalrightsfoundation.pk)	Surveillance, access inequalities, pressure on speech	Privacy preserving verification, community data, alternative comms
Southeast Asia and Pacific	Active civil society, intense online harassment, climate driven outages	EngageMedia (https://engagemedia.org), Pacific Digital Rights Observatory, mesh pilots in Fiji and Vanuatu	Disinformation, harassment, fragile connectivity	Crisis ready infrastructure, multilingual AI datasets
Europe	Most developed public interest digital ecosystem, strong regulatory frameworks	Eurosky (https://eurosky.eu), Decidim (https://decidim.org), Matrix (https://matrix.org)	latform dependency, political fragmentation	Federated services, public interest social networks, open governance

Part IV.
Gaps, Risks and Opportunities

4.1 Gaps in the Global Digital Civil Society Ecosystem

Although activity is emerging in every region, the landscape has significant gaps that limit how far decentralised or community owned models can go. These gaps are structural rather than technical. They reflect uneven access, governance capacity, regional inequalities and missing infrastructure layers that civil society cannot fill alone.

A major gap is **local hosting and operational capacity.** Many organisations rely entirely on foreign cloud providers because domestic infrastructure is either unaffordable or unavailable. This creates dependency and makes it difficult to run federated services, resilient communication tools or community governed platforms at meaningful scale.

There is also a gap in **language and data representation.** Most AI and digital tools continue to prioritise English and a small number of dominant global languages. Projects like Masakhane show what is possible, but the coverage is still limited when compared to the scale of linguistic diversity in Africa, South Asia and Southeast Asia.

Governance capacity is another missing layer. Even where open or decentralised tools exist, many organisations lack the time or expertise to participate meaningfully in their governance. Without stable multi stakeholder structures, most projects depend on small volunteer teams or short-term grants, which makes them fragile.

A fourth gap lies in **sustainable funding**. The vast majority of commons-based infrastructure is maintained by under resourced teams, small cooperatives or volunteer groups. These projects do not fit comfortably into traditional donor cycles, and few funders are set up to support long term infrastructure stewardship.

Finally, there is a gap in **regional coordination**. Many initiatives are working on similar problems, often in isolation. Efforts in Africa, Latin America, South Asia and Europe rarely intersect, even when they share technical foundations. The result is duplication, fragmented standards and missed opportunities for shared learning.

These gaps do not indicate a lack of potential but they do highlight the conditions that need to be addressed before participatory, decentralised and community owned models can operate reliably across global civil society. The next section looks at how these gaps create specific risks and what they imply for organisations that may adopt or depend on such systems.

4.2. Duplication, Fragmentation and Coordination Risks

The emerging ecosystem is energetic but fragmented. Many projects are being built in parallel, often without clear awareness of each other, and often solving similar problems with incompatible approaches. This creates duplication of effort and makes it difficult for civil society to choose reliable pathways.

One coordination challenge comes from the growing number of decentralised or federated tools that share underlying principles but lack shared standards. ActivityPub servers may operate differently from one another. Governance tools labelled as DAOs vary widely in design. Participatory platforms fork repeatedly without long term alignment. The result is innovation without convergence.

There is also a pattern of **pilot proliferation**. Organisations run isolated experiments that do not survive beyond the project cycle. Each pilot generates insight, but the learning rarely transfers to the wider ecosystem. Without mechanisms for consolidation, knowledge becomes siloed and resources spread thinly.

A further risk lies in **regional isolation**. African, Latin American, European and Asian initiatives often evolve separately even when they address the same needs, such as multilingual AI, secure communication or public interest hosting. This limits interoperability, slows down the creation of shared norms and increases the burden on civil society groups trying to navigate their options.

Finally, fragmentation creates a trust problem. When tools are unfamiliar, short lived or poorly documented, organisations hesitate to adopt them. This slows uptake and reinforces reliance on commercial platforms, even when alternatives exist.

These risks do not undermine the value of experimentation. They underline the need for coordination structures, shared reference points and strategic choices about what should be built, supported or linked together. The next section looks at how CIVICUS could help shape this in practical ways.

4.3 Strategic Opportunities for Civil Society

CIVICUS and similar civil society organisations are well-positioned to help bring coherence to an ecosystem that is inventive but scattered. The mapping in previous sections shows that many promising initiatives exist, but most lack the networks, legitimacy or long-term support needed to become stable infrastructure for civil society. Civil Society can play several practical roles that do not require building technology, but focus instead on convening, alignment and stewardship.

A clear opportunity lies in **connecting parallel effort**s. Many regional initiatives are working on related challenges, from public interest social networks to community data and crisis ready tools. Civil Society could help create shared reference points, facilitate cross regional conversations and make it easier for practitioners to learn from one another rather than working in isolation.

There is also space to support **standards and governance alignment**. Projects built on open protocols often struggle with coordination. Identify where civil society needs common approaches, whether for verification, safety, governance or interoperability, and support the development of frameworks that reduce fragmentation.

A further opportunity involves **capacity and literacy**. Many organisations are interested in alternative digital infrastructure but lack the knowledge to evaluate options or participate in governance. Develop accessible guidance, peer networks and training that give groups the confidence to engage.

Finally, there is scope to act as a **steward or anchor partner** for specific public interest tools that have clear relevance to global civil society. This does not mean owning infrastructure, but helping to support governance, convene users and ensure that the needs of civic actors are represented in key decision making spaces.

These opportunities are not directives. They are areas where Civil Society could add value in a field that is expanding rapidly but still lacks the structures needed to translate early experimentation into sustainable, widely used digital public goods.

Part V.
Action Framework

5.1 Organisational Readiness and Maturity

Civil society organisations vary widely in their ability to adopt or influence new digital infrastructure. Some already have strong technical capacity, internal governance structures and experience with open tools. Others operate with limited bandwidth, very small teams or external constraints that make even small technology shifts difficult. Readiness is not about size or budget. It is about how an organisation manages risk, makes decisions and adapts to change.

A useful way to think about readiness is to look at three dimensions. The first is governance. Organisations need clear decision making processes when adopting new tools, especially those that involve community stewardship or data handling. Without this, even promising technologies become burdensome.

The second dimension is capacity, which includes both technical skill and the ability to engage with unfamiliar governance models. Organisations rarely need deep engineering expertise, but they do need enough understanding to evaluate tools, ask the right questions, scope projects and identify risks.

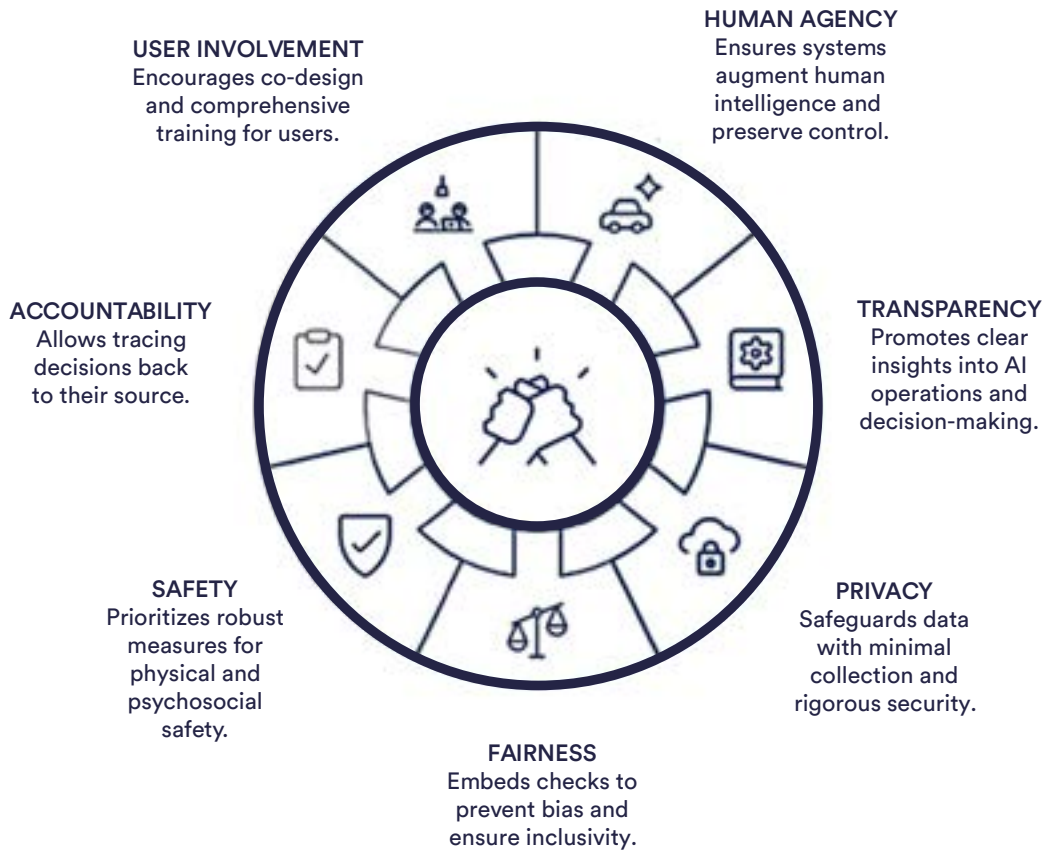
The final dimension is flexibility. Some organisations are able to experiment, adjust workflows or run parallel processes while learning. Others need stability above all else, often because of legal, political or funding pressures. This affects which models are realistically adoptable.

Taken together, they form a simple maturity curve. At the base are organisations that depend entirely on commercial platforms and lack the capacity to evaluate alternatives. In the middle are groups that can test community governed tools in limited contexts. At the top are organisations able to participate in governance, contribute to shared infrastructure or anchor parts of emerging ecosystems.

5.2 Ethical, Inclusive and Safe Design Principles

Many of the technologies now available to civil society carry trade-offs that are not always obvious at first glance. Some reduce risk but introduce new forms of dependency. Others improve accessibility yet strain organisational capacity. Given this complexity, it can be helpful to surface a small set of principles that highlight the considerations most likely to shape outcomes.

Trust by Design is a framework of principles and practices intended to ensure that collaborative intelligence systems are developed and deployed in ways that inherently foster trustworthiness and ethical behavior, in line with our second research question. The framework, whose core principles are outlined in the guide below is inspired by the concept of "Ethics by Design", integrating ethical reasoning capabilities and considerations into technology from the earliest stages, but focusing specifically on building trust as the outcome of ethical alignment.



Trust by design framework: core principles.

Principle	What It Means in Practice	Why It Matters	Key Risks if Ignored
Minimal Data Collection	Only gather what is essential for the task. Avoid sensitive identifiers unless absolutely required.	Reduces exposure, complies with rights-based norms, lowers harm in case of breach.	Data leaks, surveillance, targeting of activists, regulatory liability.
Safe Defaults	Privacy, encryption and safety settings should be enabled automatically rather than requiring user action.	Protects high risk users who may not have technical expertise.	Users remain exposed by accident, inconsistent protection across teams.
Accessibility by Design	Works with low bandwidth, older devices, screen readers, multiple languages.	Ensures participation is possible across regions, abilities and connectivity levels.	Excludes rural communities, disabled users, low income participants.
Transparency of Rules and Changes	Clear documentation of moderation, data use and governance. Notice before major changes.	Builds trust and reduces dependency on opaque actors.	Sudden disruptions, loss of control, inability to contest decisions.
Independent Oversight	Governance includes external or community voices who can question decisions.	Prevents concentration of power and strengthens legitimacy.	Abuse of authority, biased decision making, unaccountable operations.
Interoperability and Open Standards	Can connect to other tools and move data safely between systems.	Reduces lock-in and increases resilience.	Technical or legal dependency on a single provider.
Contextual Safety	Designed to reflect local risks, including surveillance, gendered harassment and repressive laws.	Recognises that threats differ by region and community.	A tool that is safe in one country may be dangerous in another.
Revocability and Exit	Users can leave, delete data or migrate without penalty.	Protects autonomy and prevents coercive lock-in.	Organisations become trapped in systems they cannot exit.
No Hidden Incentives	Business model, funding and sustainability are clear.	Ensures values are aligned with public interest, not extractive incentives.	A “free” tool may depend on data extraction or advertising.
Inclusive Governance	Affected communities have a role in decision making and dispute resolution.	Aligns with civil society values and improves long term viability.	Marginalised communities excluded from rule setting, reinforcing inequities.

Practical Considerations

Conditions for Safe and Effective Adoption

Before considering any new infrastructure or governance model, it is essential also to recognise the conditions under which civil society organisations actually operate. Many face political pressure, inconsistent funding, fragile staffing arrangements and limited digital capacity. Others work in environments where connectivity is unreliable or where adopting the wrong tool can place people at real risk. These variations mean that the ability to adopt new systems is not determined by interest or intent, but by the practical realities surrounding an organisation. Understanding these conditions is therefore a prerequisite for any responsible approach to digital transformation.

Condition	What It Looks Like in Practice	Why It Matters	Risks if Missing
Organisational Stability	Basic internal clarity on roles, decision-making and risk ownership during digital change.	Prevents adoption decisions being driven by crisis or staff turnover.	Fragmented decisions, poorly managed risk, stalled initiatives.
Minimum Digital Capacity	Someone in the organisation can evaluate safety, governance and sustainability of tools. Not a technical expert, but a confident evaluator.	Ensures tools are chosen intentionally, not reactively.	Adoption of unsafe or unsuitable systems.
Political Feasibility	Technology choices do not expose staff or communities to surveillance, legal pressure or retaliation.	Essential for organisations in restrictive civic spaces.	Heightened threat levels, criminalisation, exposure of participants.
Resource Predictability	Time, budget and staff continuity to adopt or test tools without overextending.	Allows for gradual, low-risk experimentation.	Organisations abandon tools mid-way or create dependency on volunteers.
Connectivity Baseline	Tools function under real-world conditions: unstable bandwidth, shared devices, low-spec hardware.	Many contexts still operate on 2G/3G or intermittent access.	Exclusion of rural and low-income communities; system failure during crises.
Peer Support	Access to regional or thematic networks for troubleshooting, safety advice and governance guidance.	Civil society rarely succeeds with digital adoption alone.	Knowledge gaps, duplicated mistakes, isolation.
Exit Options	Ability to leave or migrate from a tool without losing data or community trust.	Avoids lock-in, protects autonomy.	Dependence on vendors, platforms or infrastructure outside the sector.
Cultural Fit	Technology aligns with organisational values, workflows and community expectations.	Tools that clash with organisational culture fail even when technically sound.	Low uptake, friction, quiet abandonment.

5.3. Funding Models for Shared Infrastructure

Digital public infrastructure only becomes reliable when the funding behind it is reliable. Many of the systems that civil society depends on today emerged from volunteer labour, small grants or short bursts of institutional enthusiasm, and the result is an ecosystem where critical tools often sit on unstable foundations. The organisations that have endured the longest tend to be those that found sustainable models early. Mozilla's long running support for open source is an example. Through the Mozilla Open Source Support programme, the organisation has channelled institutional and philanthropic resources into essential internet tools for nearly a decade, providing one of the few dependable funding anchors for shared digital goods.

A different approach can be seen in Barcelona's stewardship of Decidim, the open source participation platform. Decidim is funded and governed as part of the city's democratic infrastructure rather than as a standalone tech project. This gives it a degree of durability that most civic tech tools never achieve. The project's governance model includes community representation, transparent decision making and long term planning, all supported by municipal commitment. It shows how public institutions can sustain digital commons at scale when funding, governance and mission align.

Other models distribute the burden more widely. Open Collective allows community groups, grassroots networks and open source teams to receive and manage funds through a shared fiscal hosting structure. Instead of each group building its own administrative machinery, Open Collective provides transparency, accounting and governance support, funded through small fees from participating organisations. This cooperative model has become a backbone for hundreds of civil society and open source communities that would otherwise struggle with basic financial infrastructure.

Hybrid models are also emerging. The Matrix Foundation, which oversees the Matrix communication protocol, blends institutional adoption, philanthropy and community support. Matrix is used by governments, NGOs and public sector bodies across Europe, and this diversity of users has helped spread responsibility for its long term maintenance. The Open Tech Fund sits in a similar space, providing globally distributed funding for security tools, censorship circumvention and open infrastructure used by journalists, activists and civil society groups under pressure. Both cases illustrate that resilient infrastructure rarely depends on a single funding stream. It is sustained through a network of institutions, funders and users who share responsibility over time.

A growing number of projects also explore blockchain based or DAO-enabled funding mechanisms for public digital goods. These systems treat infrastructure as a shared resource and use transparent on-chain treasuries or community voting to allocate maintenance budgets. They allow for continuous, small scale contributions from a wide pool of stakeholders rather than relying solely on grants or public procurement. This approach remains experimental and is not suitable for every context, but it offers lessons on how funding, governance and long-term maintenance can be tied together in a more predictable and accountable way.

Model	How It Works	Strengths	Risks	Links
Pooled Philanthropy	Multiple donors jointly support maintenance, hosting and governance.	Stability, shared responsibility.	Coordination overhead; shifting donor priorities.	Mozilla Open Source Support (https://www.mozilla.org/en-US/moss/), Open Tech Fund (https://www.opentech.fund/about/)
Public / Municipal Funding	Governments fund or host civic digital infrastructure.	Scale, institutional durability.	Vulnerable to political change or budget cycles.	Decidim governance (https://decidim.org/governance/), French DINUM open source policy (https://code.gouv.fr)
Membership / Cooperative Models	Organisations pay small recurring fees and share governance.	Predictable revenue; aligned incentives.	Harder in low-resource regions; requires coordination.	Open Collective fiscal hosting (https://opencollective.com/foundation), Hypha Worker Co-op (https://hypha.coop/about/)
Hybrid Models	Mix of public, donor and community support.	Balanced, adaptable.	Governance complexity.	Matrix Foundation funding model (https://matrix.org/foundation/)
Institutional Procurement	Public bodies adopt and budget for open tools.	Long-term continuity through service contracts.	Procurement rules may exclude smaller projects.	EU ActivityPub adoption context (https://joinfediverse.wiki/European_Union)
Volunteer / Donation Only	Community maintains infrastructure without formal funding.	Fast to launch; values-driven.	Unsustainable for critical services; burnout risks.	Mastodon server sustainability notes (https://docs.joinmastodon.org/admin/scaling/)
DAO or On-Chain Public Goods Funding	Distributed contributors fund shared infrastructure through on-chain treasuries and governed allocations.	Transparency, continuous micro-funding and community ownership.	Volatile in low-trust or low-liquidity environments.	Gitcoin grants model: https://gitcoin.co. Optimism RetroPGF: https://www.optimism.io/retroPGF.

5.4 Transformation Framework for Civil Society Digital Infrastructure

Civil society organisations use technology under conditions that are frequently unstable, under-resourced and politically constrained. Some are trying to stay online during repeated shutdowns; others are adapting to rapid regulatory shifts; many operate with minimal technical capacity and rely on tools chosen for convenience rather than strategy. These realities mean that any attempt to talk about "transformation" has to be grounded in the way organisations actually work. Most do not have the luxury of long planning cycles, and many have to make decisions under pressure.

Despite this complexity, patterns are emerging. Across regions, organisations are gradually developing shared practices, forming informal clusters of experimentation and building pockets of capability that make it easier to evaluate new systems. None of this is uniform, and it will not evolve at the same pace everywhere. But taken together, these patterns offer a way to think about transformation that reflects the uneven terrain civil society navigates.

These patterns of transformation describe what is helping organisations strengthen their digital autonomy (without assuming that decentralisation or new infrastructure will suit every context). Some organisations move cautiously, others more quickly. Furthermore, political constraints often define what is possible in many places. What matters is not adherence to a model, but creating conditions in which organisations can act with greater confidence, safety and collective resilience.

Transformation, in this sense, is not about adopting specific tools. It is about building the capacity to make informed choices, supporting the networks that already produce context-appropriate solutions, and ensuring that the infrastructure civil society depends on is not entirely shaped by actors outside the sector.

For example…

Component	What It Means	Why It Matters
Shared Foundations	Light, widely applicable practices that reduce harm and simplify collaboration across varied contexts.	Creates a baseline for safety and interoperability without requiring new technology or high capacity.
Regional and Thematic Clusters	Support for networks already experimenting with tools shaped by local conditions.	Encourages learning across contexts, reduces duplication and respects regional diversity.
Capability Building	Practical literacy that helps organisations judge risks, governance models and long-term implications.	Enables informed decision making and reduces hesitation around unfamiliar systems.
Stewardship and Anchors	Stable institutions (where they exist) that can maintain documentation, governance and continuity over time.	Helps infrastructure outlast funding cycles, staff turnover and political disruption.

Part VI.
Tools, Glossary and References

6.1 Practical Tools & Infrastructure Table

(These are not specific recommendations — they are reference points across the ecosystem.)

Category	Tool / Project	What It Is / Why It Matters	Link
Secure Communication	Signal	End-to-end encrypted messaging; widely adopted by civic actors.	https://signal.org
	Matrix	Federated communications protocol; used by governments and NGOs; self-hostable.	https://matrix.org
	Element	Leading Matrix client; secure collaboration platform.	https://element.io
	Cwtch	Peer-to-peer encrypted group messaging with no central server.	https://cwtch.im
	Session	Decentralised, onion-routed messaging; minimal metadata.	https://getsession.org
Participation & Governance Platforms	Decidim	Open-source participation platform with rigorous governance model.	https://decidim.org
	Pol.is	Structured conversation analysis used in Taiwan and global deliberation pilots.	https://pol.is
	Loomio	Lightweight, accessible decision-making for groups & collectives.	https://loomio.org
	Your Priorities	Community consultation platform built by the Citizens Foundation (Iceland).	https://yrpri.org
	vTaiwan Models	Frameworks for digitally augmented deliberation; widely studied.	https://vtaiwan.tw
Identity / Verification / PoP	BrightID	Social graph identity; Proof-of-personhood via attestations.	https://brightid.org
	Proof of Humanity	Crowdsourced video-based verification; governance experimentation.	https://www.proofofhumanity.id
	Worldcoin (critical reference)	Biometric PoP system; controversial but influential — included for landscape completeness.	https://worldcoin.org
	Mozilla Digital Credentials	Standards work on decentralised identity and verifiable credentials.	https://github.com/w3c/vc-data-model
Community Data & Open AI Ecosystems	Masakhane	Pan-African NLP research community; open datasets & models.	https://masakhane.io
	Hugging Face	Open model ecosystem; transparency tools; dataset governance.	https://huggingface.co
	LatinX NLP	Regional community for inclusive language tech.	https://latinxnlp.org
	BigScience BLOOM	Open multilingual large language model; global research collaboration.	https://huggingface.co/bigscience/bloom

Category	Tool / Project	What It Is / Why It Matters	Link
Digital Public Infrastructure (Global)	GovStack	Modular open standards for public service components.	https://www.govstack.global
	India Stack	Identity, payments, and data layers underpinning DPI models.	https://www.indiastack.org
	MOSIP	Open-source identity for governments; adopted in multiple countries.	https://mosip.io
	Estonia X-Road	Interoperability backbone; widely studied.	https://x-road.global
Public Interest Social Infrastructure	Eurosky	Emerging European public-interest social network (early-stage).	https://eurosky.eu (placeholder)
	Mastodon	Federated social networking; widely adopted post-Twitter.	https://joinmastodon.org
	PeerTube	Decentralised video hosting; ActivityPub compatible.	https://joinpeertube.org
	Bluesky AT Protocol	Open social protocol; decentralisation trajectory.	https://bsky.app
Collective Governance & Resource Sharing	Open Collective	Transparent funding & fiscal hosting for communities.	https://opencollective.com
	Giveth	Community-governed funding ecosystem for social impact projects.	https://giveth.io
	Aragon	Modular on-chain governance tools (used beyond blockchain contexts conceptually).	https://aragon.org
	Hypha Co-op	Worker cooperative offering digital governance & infra stewardship models.	https://hypha.coop
Low-Connectivity / Crisis-Ready Tools	Briar	Messaging via Bluetooth/WiFi without internet.	https://briarproject.org
	goTenna	Off-grid mesh communication hardware.	https://gotenna.com
	Bridgefy*	Bluetooth mesh messaging (note: previous security concerns).	https://bridgefy.me
	IPFS	Distributed storage; used in crisis for resilient content hosting.	https://ipfs.tech
	OONI	Monitoring censorship and network interference globally.	https://ooni.org
Hosting, Websites & Ops	WordPress.org	The most widely used open-source CMS; adaptable across contexts.	https://wordpress.org
	Netlify CMS	Git-based content management for low-ops teams.	https://www.netlifycms.org
	Cloudron	Easy self-hosting layer for dozens of OSS apps; used by small NGOs.	https://cloudron.io
	Nextcloud	Self-hostable file sharing/collaboration suite; popular in EU civic contexts.	https://nextcloud.com

Category	Tool / Project	What It Is / Why It Matters	Link
Security & Safety	Security First: Umbrella	Digital & physical security field manual for activists.	https://securityfirst.org
	Access Now Helpline	Rapid digital security support for at-risk groups.	https://www.accessnow.org/help
	Redact	Removes exposed personal data from the open web.	https://redact.dev
	Scrutineer	Automated scans for doxxing exposure.	https://scrutineer.dev
Deliberation Support & Collective Sensemaking	Polis	Used in Taiwan, Canada, EU for large-scale deliberation.	https://pol.is
	Your Priorities	Community idea generation & debate platform.	https://yrpri.org
	Kialo	Structured arguments; sometimes used by NGOs for internal learning.	https://www.kialo.com
Mapping, Open Knowledge & Commons	Wikipedia + Wikimedia Ecosystem	Community-owned global knowledge infrastructure.	https://wikimediafoundation.org
	OpenStreetMap	Global open mapping; widely used in crisis response and development.	https://www.openstreetmap.org
	Framasoft	French public interest tech collective offering decentralised tools.	https://framasoft.org
Digital Rights Monitoring	SMEX	Digital rights & platform accountability in MENA.	https://smex.org
	7amleh	Palestinian digital rights; platform accountability reports.	https://7amleh.org
	Derechos Digitales	Latin America digital rights research.	https://derechosdigitales.org

6.2 Glossary

A

- **ActivityPub**
  An open protocol that allows different social platforms to interact with one another. Used by Mastodon, PeerTube and other “Fediverse” services.

- **Anchor Institution**
  A stable organisation — such as a university, established NGO or cooperative — that can maintain governance processes, documentation and continuity for shared digital tools or standards.

- **API (Application Programming Interface)**
  A way for different software systems to communicate. Changes to commercial APIs often disrupt NGO workflows that depend on them.

- **AT Protocol**
  The decentralised social networking protocol used by Bluesky. Designed to allow multiple hosts and portable user identities.

B

- **Blockchain**
  A type of shared ledger maintained across many computers. Provides transparent record-keeping, but is not inherently democratic or decentralised.

C

- **Civic Tech**
  Technology used to support participation, transparency, public engagement or collective decision-making. Varies widely by region and context.

- **Community Network**
  Locally built and governed internet infrastructure, often used in rural or underserved areas. Designed to increase connectivity autonomy.

- **Crisis-Ready Tools**
  Technologies that continue functioning during outages, shutdowns or low-bandwidth conditions. Examples include mesh messaging apps and offline-first tools.

D

- **DAO (Decentralised Autonomous Organisation)**
  A broad term for digital governance structures where decisions and shared resources are managed through transparent rules encoded in software. Quality and purpose vary significantly.

- **Data Minimisation**
  The practice of collecting only the information needed to perform a task. Reduces risk for organisations working with vulnerable communities.

- **Decentralised Identity (DID)**
  Identity systems that allow people to control their own credentials rather than relying on central authorities.

Glossary

D

Decidim
An open-source platform for democratic participation originally developed in Barcelona. Known for its transparent, multi-stakeholder governance model.

Digital Commons
Shared digital resources — such as software, data or platforms — governed collectively rather than owned privately.

Digital Public Infrastructure (DPI)
Core digital systems for public services, such as identity, payments or data exchange. Approaches differ by region and governance model.

Distributed / Federated System
A system that runs across many servers or operators instead of a single central provider. Allows communities or institutions to host their own instances.

E

Encryption
A method of securing communication so only the intended recipient can read it. Essential for protecting sensitive conversations.

F

Fediverse
A group of interoperable social platforms (such as Mastodon and PeerTube) that communicate using ActivityPub. No single company owns the network.

G

Governance Layer
The rules, decision-making processes and accountability mechanisms that define how a system is run — independent of its technical design.

GovStack
A modular approach to building public digital services using open standards. Helps countries avoid vendor lock-in.

I

IPFS (InterPlanetary File System)
A distributed storage protocol that allows content to be hosted across many nodes rather than a central server.

M

Mesh Network
A network where devices connect directly to one another, allowing communication when traditional infrastructure is unavailable.

Metadata
Information about a communication (such as time, location, device) rather than its content. Often more revealing than the message itself.

Glossary

O

Open Data
Data that is accessible, reusable and shared openly, usually with clear licensing. Important for transparency and research.

Open Source Software
Software whose code is publicly accessible and can be inspected, modified or shared. Governance varies widely.

P

Participation Platform
A digital tool used for consultations, deliberation, idea-sharing or collective decision-making.

Peer-to-Peer (P2P)
A model where devices communicate directly with each other rather than via a central server.

Proof of Personhood (PoP)
Methods for confirming that someone is a real, unique human without revealing their full identity. Approaches include social verification, video challenges and biometrics.

R

Resilience (Digital)
The ability to continue operating during outages, shutdowns, platform changes or other disruptions.

S

Self-Hosting
Running software on an organisation's own server or infrastructure rather than relying on a commercial provider.

Stewardship
Long-term care and governance of tools, standards or infrastructure, often shared across multiple organisations.

V

Verification (Digital)
Ways to confirm that a user, message or participant is genuine. Methods range from social trust to device checks to cryptographic proofs.

W

Web3 (Contextual Definition)
A broad set of technologies that aim to distribute control of digital systems, typically using blockchains or decentralised protocols. Quality and purpose vary significantly by project.

6.3 References

Civil Society, Digital Rights & Platform Governance

CIVICUS Monitor. "Tracking Civic Space Worldwide." 2024–2025.
https://monitor.civicus.org

UN Human Rights Council. "Reports of the Special Rapporteur on Freedom of Peaceful Assembly and Association." 2024.
https://www.ohchr.org

Access Now. "The State of Internet Shutdowns 2024."
https://www.accessnow.org/internet-shutdowns

Digital Defenders Partnership. "Digital Threats & Protection for Human Rights Defenders." 2024.
https://digitaldefenders.org

The Engine Room. "Understanding Digital Capacity in Civil Society." 2024.
https://theengineroom.org

Mozilla Foundation. "Internet Health Report." 2024–2025.
https://foundation.mozilla.org

SMEX. "Regional Digital Rights Reporting (MENA)."
https://smex.org

7amleh. "Palestinian Digital Rights Reports."
https://7amleh.org

Derechos Digitales. "Annual Latin America Digital Rights Review."
https://derechosdigitales.org

Public Interest Digital Infrastructure (DPI)

GovStack. "Building Digital Public Infrastructure with Open Standards." 2023–2025.
https://govstack.global

Digital Public Goods Alliance. "Digital Public Goods Registry."
https://digitalpublicgoods.net

India Stack. "Digital Public Infrastructure for Identity, Payments, Data."
https://indiastack.org

MOSIP. "Modular Open Source Identity Platform."
https://mosip.io

Estonia X-Road. "Interoperability Framework."
https://x-road.global

European Commission. "Digital Services Act and Digital Governance Programmes." 2024.
https://digital-strategy.ec.europa.eu

Eurosky Project (Early Development Reference).
https://eurosky.eu (placeholder / early-stage)

Federated & Decentralised Social Infrastructure

W3C. "ActivityPub: Protocol for Decentralised Social Networking."
https://www.w3.org/TR/activitypub

Mastodon. "Fediverse Social Networking."
https://joinmastodon.org

PeerTube. "Decentralised Video Hosting."
https://joinpeertube.org

Bluesky / AT Protocol.
https://atproto.com

Framasoft. "Public-Interest Digital Services."
https://framasoft.org

References

Participation, Deliberation & Governance

Decidim. "Participatory Democracy Platform & Governance Model."
https://decidim.org

Pol.is. "Large-Scale Digital Deliberation."
https://pol.is

Your Priorities (Citizens Foundation Iceland).
https://yrpri.org

Loomio. "Collaborative Decision-Making."
https://loomio.org

vTaiwan Digital Democracy Initiative.
https://vtaiwan.tw

Aragon. "Modular Governance Frameworks."
https://aragon.org

Giveth. "Community-Driven Governance and Funding."
https://giveth.io

Open Collective. "Transparent Fiscal Hosting Infrastructure."
https://opencollective.com

Hypha Worker Co-operative.
https://hypha.coop

WEF. "Decentralized Autonomous Organization (DAO) Toolkit." 2023.
https://www.weforum.org/publications/decentralized-autonomous-organization-toolkit

Identity, Human Verification & Proof of Personhood

BrightID. "Social Graph Identity Verification."
https://brightid.org

Proof of Humanity.
https://proofofhumanity.id

Worldcoin.
https://worldcoin.org

W3C. "Verifiable Credentials Data Model."
https://www.w3.org/TR/vc-data-model

Mozilla. "Digital Credentials Working Papers."
https://github.com/w3c/vc-data-model

Polkadot - proof of personhood/individuality protocol
https://polkadot.com/blog/proof-of-personhood-polkadot-project-individuality/

References

Community Data, Inclusive AI, and Open Models

Masakhane. "African Natural Language Processing (NLP)."
https://masakhane.io

LatinX NLP.
https://latinxnlp.org

Hugging Face. "Open Models & Transparency Tools."
https://huggingface.co

BigScience Project / BLOOM Model.
https://huggingface.co/bigscience/bloom

IDRC. "Inclusive AI and Digital Resilience."
https://idrc.ca

GSMA. "Mobile Internet Connectivity Report 2024."
https://www.gsma.com/mobilefordevelopment

UN Broadband Commission. "Connectivity & Inclusion Reports."
https://www.broadbandcommission.org

Safety, Security & Crisis Infrastructure

Signal Foundation.
https://signal.org

Matrix Foundation.
https://matrix.org

Element (per your request — all relevant links):

Main site: https://element.io
Documentation: https://element.io/help
Security overview: https://element.io/security
Open source repository: https://github.com/vector-im

Cwtch.
https://cwtch.im

Session.
https://getsession.org

Briar.
https://briarproject.org

goTenna.
https://gotenna.com

OONI – Open Observatory of Network Interference.
https://ooni.org

IPFS – InterPlanetary File System.
https://ipfs.tech

Security First – Umbrella.
https://securityfirst.org

Access Now Helpline.
https://www.accessnow.org/help

Scrutineer.
https://scrutineer.dev

Redact.
https://redact.dev

References

Knowledge & Commons Ecosystem

Wikimedia Foundation.
https://wikimediafoundation.org

OpenStreetMap.
https://openstreetmap.org

Creative Commons.
https://creativecommons.org

Hosting, Websites, and Self-Managed Ops

WordPress.org
https://wordpress.org

Netlify CMS
https://www.netlifycms.org

Nextcloud
https://nextcloud.com

Cloudron
https://cloudron.io

civicus.org

humanfuture.agency