dComms Final Report

Table of content

1) Intro about the project

The dComms project is a research-led initiative focused on testing and deploying communication tools that can withstand difficult digital environments. While we often think of the internet as a global, open space, the reality for many is a landscape of heavy censorship, constant surveillance, and the threat of total network shutdowns. For journalists, activists, and vulnerable communities, relying on major corporate platforms often means being vulnerable to data mining, government monitoring, or being blocked without warning.

dComms was created to research how decentralized, community-owned infrastructure can provide a more resilient alternative.

Instead of just looking for ways to jump over a firewall, we focused on helping communities build their own independent communication setups - systems that are censorship-resilient and surveillance-resistant by design. By using Fediverse tools like Mastodon and Matrix, we helped local partners set up their own independent communication servers. Because these servers are hosted locally, they can keep running even when the rest of the global internet is cut off. It's about moving away from the Big Tech model and toward a community-owned model—where the people using the tools are the ones who actually own the infrastructure.To test this idea in the real world, we decided to work with five partners across five different regions, each facing its own unique set of challenges;

- Colnodo in Colombia
- Redes in Mexico
- CITAD in Nigeria
- SMEX in Lebanon
- Delo LGBT+ in Russia

By spreading our focus across these diverse locations, we wanted to see if decentralized tools could be adapted to fit different community needs, legal risks, and technical landscapes.

This past year has been a massive experiment in resilience. This report is our look back at that experience. We've gathered the data, listened to the feedback from the people on the ground, and documented the hard lessons we learned about what it really takes to keep a community connected when their connection to the outside world is cut off.

2) Summary of Overall Impact

The dComms project served as a vital real-world laboratory for testing how communities can transition from centralized Big Tech to the Fediverse. Our findings indicate that while technical sovereignty is achievable, it is not a standalone driver for community movement. We successfully proved that decentralized infrastructure can provide a vital lifeline and a powerful shield in shutdown-resilient and censorship-heavy circumstances, but these technical victories only translate into sustained adoption when the technology aligns with the physical and social realities of the users.

The project revealed that the transition to the Fediverse is primarily gated by habit and technical friction. We observed that users do not choose tools based on privacy alone; they prioritize platforms that are already inhabited by their community and are easy to access without expert guidance. The challenges in the pilot highlighted that if decentralized tools remain heavier and less optimized than commercial apps, the technical overhead becomes a primary obstacle to long-term adoption.

Ultimately, dComms shifted the mindset of our international partners toward digital sovereignty, providing them with the tools to manage their own digital spaces. The project proved that the technology remains operational even when external connections are severed, but the next stage of development must focus on the human interface. For the Fediverse to become a practical alternative for mass adoption, the future of decentralized tech must be lighter, more efficient, and designed with a friction-free onboarding process. We have built the resilient infrastructure for these specific circumstances; the task now is to ensure the transition is as seamless and intuitive as the platforms people are currently using.

3) Impact Evaluation: Testing our 5 Hypotheses in Real-World Scenarios

The dComms project was designed to test five key hypotheses regarding the specific conditions that encourage communities to shift their digital presence from centralized Big Tech platforms to the Fediverse. Below is an evaluation of which circumstances successfully fostered this transition and which created hurdles for adoption.

1. The Need for Shutdown Resilient Communications

the first hypothesis was to test if the promise of staying online during a total internet shutdown would be a primary driver for communities to adopt a local-first network. Because these tools do not rely on a single central data center, they are much harder to turn off with a single switch. While the local servers remained operational throughout our testing, we learned that a technical success does not always translate to a social one; many users felt that if they could not reach the wider world, the local network felt too quiet to sustain their daily activity.

We found that a local network is only truly useful if a large community is already using it as a habit before a shutdown occurs. This was proven in Nigeria by CITAD, where a solar-hybrid server remained functional as a local communication island. This case demonstrated that the technology remains alive even when the global internet is cut off, providing a vital lifeline for local coordination. Ultimately, this validated that while the technology stays running even when the rest of the world is cut off, the transition is most successful when the tool is already integrated into the community's daily life.

2. The Need for Censorship Resilient Communications

We hypothesized that the desire to escape government blocking would drive users to transition toward decentralized tools. Unlike mainstream apps that have one front door that can be locked, dComms allows for many entry points, creating a resilient shield against state-level censorship. In Russia, the development of the Telegram-to-Mastodon bridge by Delo was a key success in testing this strategy, as it allowed users to keep their existing audience while proving their core data to a safer space.

This foot in both worlds approach proved that decentralization is a powerful shield against state-level censorship, provided the technical solution is paired with a safe way for the community to engage.

While the technical bridge was a success, stronger evidence of a full community shift requires future testing that prioritizes a properly executed outreach strategy.

3. The Need for Local-First Services in Rural Geographies

This hypothesis was the most difficult to prove, especially based on feedback from Colombia and Nigeria. We believed that a local mini internet would be the perfect solution for rural areas, but the reality of bad connectivity and low bandwidth created a major barrier. Many of the tools we used are heavy and require a constant, stable stream of data just to open. In rural Colombian villages and remote parts of Nigeria, where users rely on weak signals and older phone models, the apps frequently timed out or crashed before they could even load a message.

We also found that even when a local server is running perfectly,the final connection to the user's device often fails if the bandwidth is too low. Because these decentralized tools are not yet optimized for low-resource environments, they struggle to perform in the very places that need them most. The project taught us that for local-first services to work, they cannot just be local; they must also be built specifically for low-bandwidth reality and unreliable power.

4. The Need for Community Ownership of Infrastructure

The idea that owning the server leads to better privacy was correct, but we found a significant financial barrier in Mexico. While owning the infrastructure protects users from being watched, the data hunger of these tools is a major problem for sustainability. In Mexico, where mobile data is very expensive and often sold in small packages, users found that Fediverse tools consumed their data plans much faster than mainstream apps like Telegram or WhatsApp. This is because these decentralized platforms often download more metadata and media in the background than commercial apps that have been highly optimized for years.

This creates a difficult choice for activists and community members. Even if they trust their own community server more than a corporate one, the high cost of data makes it difficult for people to actually use the service for their daily needs. We observed that users would often switch back to commercial apps simply because they could not afford the data required to stay connected to the dcomms tools. This feedback validated that while true security depends on community ownership, owning the building is not enough if the cost of entering that building is too high.

To fully understand the potential of community ownership, additional testing is required in contexts where data prices are not a barrier. By deploying these tools in environments with affordable or unlimited data, we could determine if users would stay committed to decentralized platforms based on trust and privacy alone, or if the social dominance of

Big Tech remains the primary obstacle. For these tools to be successful in the long term, they must be redesigned to be much more data-efficient so that privacy does not become a luxury only accessible to those with expensive data plans

5. The Requirement for Easy-to-Adopt Software

This hypothesis was mostly disproven in its current state. Across all regions, including our pilots in the different countries, we learned that the software is not yet easy for the average person to use or understand. The feedback was consistent: the setup process takes too long and the technical language used in the apps is confusing for non technical users. We found that most people stop trying to use the tools at the very first step because of the friction involved in creating accounts or managing cryptographic keys.

The project revealed that a community will not shift their digital habits if the tool is difficult to open; the only successful transitions occurred when a mentor provided face-to-face support to help people make the adoption. This proves that for a successful move to the Fediverse, security and privacy cannot come at the expense of usability. Since the majority of technical hurdles occurred specifically during the onboarding and registration phases, it is likely that a dedicated feature or automated flow for this stage could fundamentally change the user experience and lead to significantly higher adoption rates.

4) Qualitative Data: Summaries from the 5 Partners

This section moves away from the numbers and looks at the soul of the project. Each partner navigated a completely different social and political landscape. Their success wasn't just in keeping a server running, but in adapting decentralized technology to solve local challenges.

Colnodo (Colombia)

Colnodo approached the dComms project with a deep focus on digital sovereignty for local communities, operating on the foundational belief that for a community to be truly resilient, it must own the digital ground its data sits on. Rather than simply providing a service, they set out to build a repeatable model, focusing heavily on rural and remote geographies where the global internet is often either unreliable or prohibitively expensive.

Their work centered on the Jxa’h Wejxa community network, a group facing significant daily risks within their territory. Colnodo’s intervention began with a rigorous risk

assessment involving interviews and baseline forms to identify specific vulnerabilities in information management. They recognized that community members were frequently exposed to unsafe digital spaces, making the deployment of dComms not just a technical upgrade, but a necessary protection of their physical and digital autonomy.

To ensure these tools were actually adopted, Colnodo developed a participatory outreach strategy based on a constructivist pedagogical model. They utilized the ADIPS approach, a five-stage framework designed to move participants from basic awareness to practical mastery:

- **Activity:** Motivational icebreakers to encourage reflection on digital needs.
- **Debate:** Contextual conversations to bridge the gap between community life and technology.
- **Information:** Interactive sessions sharing the core theories of decentralization.
- **In-depth learning:** Hands-on technical training, including the installation and configuration of software.
- **Summary:** Collaborative reviews to determine how these tools would be used in daily collective work.

The analysis of this implementation revealed a high adoption rate for Element, primarily driven by the community's demand for secure chat tool. Participants specifically valued the multi-factor authentication and end-to-end encryption. The key messaging during these sessions focused on how decentralized tools minimize the risk of data leaks and external interference. This directly validated the project's central hypothesis: that decentralization is a critical tool for privacy in sensitive, high-risk environments.

Despite the successful rollout, Colnodo identified clear hurdles for long-term continuity. The primary concern is regarding content management controls and the technical learning curve remain. Ultimately, Colnodo concluded that the survival of these networks beyond the pilot phase depends entirely on the local leadership of community managers and the continued active ownership of the tools by the people themselves.

Through this process, they discovered that local connectivity is not just about geography, but about trust. Users were far more likely to join the network because they knew the people behind Colnodo personally, proving that human relationships are the ultimate foundation of any decentralized network.

.

Redes (Mexico)

Redes took a highly disciplined, capacity-building approach, recognizing that a team must be experts themselves before they can effectively lead a community. Their strategy was grounded in a community needs assessment which identified that while censorship-resilient communication is a priority, structural limitations in mobile technology—such as location tracking and a lack of telecom transparency—cannot be solved by software alone. This led to a central insight: trust is not generated solely by encryption, but by the community's perception that the organization genuinely prioritizes their protection.

To bridge this gap, Redes created a unified project identity called "Caparazón Digital" (The Digital Shell). This identity was supported by transversal actions, including "Quick Tips" guides, visual materials to lower entry barriers, and outreach through SMS campaigns and newsletters. This approach transformed dComms from a collection of technical services into a community learning process that is now a permanent line of action within Redes.

Their onboarding strategy specifically targeted three distinct groups:

- General MVNO Users: Urban users seeking ethical alternatives.

- Community-Driven Users: Activists and human rights defenders using Element as a secure digital hub for coordination.
- Tech Enthusiasts: Allies focused on digital sovereignty and open technologies.

A key finding from their deployment was that while users are interested in security, they often struggle to complete registration or remain active on micro-blogging platforms like Mastodon due to a lack of familiarity. This has pushed Redes to explore more visually engaging alternatives for communities with digital literacy limitations. Ultimately, Redes proved that while software is the tool, the "Digital Shell" of community governance, transparency, and digital literacy is the true layer of security for defenders and Indigenous communities.

CITAD (Nigeria)

CITAD operated in some of the most challenging environments of the project, including the regions of Itas and Jama’are, which are characterized by poor connectivity and frequent infrastructure vandalism. To address these hurdles, they successfully deployed a solar-hybrid server, proving that digital resilience in the Global South is possible without reliance on a national power grid. Their approach was built on the dual hypotheses that remote geographies urgently need local-first communication services and that community ownership of infrastructure is the only way to ensure long-term stability. This technical success was amplified by strategic partnerships with major institutions like Kano Polytechnic and Premier Radio, which helped elevate the Fediverse from a niche technical project to a point of public conversation.

Their outreach strategy was rooted in physical, on-the-ground engagement, targeting students, journalists, and community-led organizations with a specific focus on gender digital inclusion. By producing and sharing illustration videos in both English and Hausa, they ensured that the technical concepts of the Fediverse were culturally and linguistically accessible. These strategic sessions allowed CITAD to work directly with local influencers to identify the specific catalysts needed to encourage migration away from Big Tech.

The results of this deployment provided critical insights into user motivation, revealing that while communities are eager for alternatives to Big Tech to avoid misinformation, the monetization policies of Big Tech platforms remain a powerful financial incentive to stay. This is largely because commercial platforms are not just social spaces but economic ones; through ad-revenue sharing, creator funds, and integrated marketplaces, they offer users a path to direct income. In regions where the digital economy is a primary source of livelihood, the financial carrot of these platforms creates a significant barrier to migration, as decentralized tools—which prioritize privacy over profit—do not yet offer a comparable way for users to monetize their content or reach a global customer base.

Ultimately, the pilot demonstrated that a six-month window is insufficient for full deployment and mass migration. While existing social media users were motivated by privacy, newcomers were attracted by the sense of community safety. CITAD's experience highlights that while the lights can stay on through solar power, building a sustainable digital community requires a long-term commitment to digital literacy and finding ways to demonstrate value that competes with the economic pull of corporate platforms.

SMEX (Lebanon)

In Beirut, SMEX operated in an environment of constant crisis, including economic collapse and political instability, which led them to adopt a model focused heavily on research and infrastructure stability. Their primary contribution was a rigorous journalist impact survey involving fifty key media figures, which provided the project with valuable data on platform inertia. This research documented the specific reasons journalists are hesitant to leave mainstream platforms and identified the exact requirements for moving professional communities to decentralized spaces. By prioritizing this research, they established that in high-stakes environments, a tool that fails is more dangerous than having no tool at all.

However, this focus on technical caution and internal research also highlighted a significant strategic trade-off regarding community outreach. Because resources were concentrated on infrastructure reliability and survey data, there was a noticeable gap in on-the-ground engagement and active recruitment of the broader community. This experience served as a critical learning point for the dComms project, demonstrating that technical excellence and rock-solid stability are not enough to drive adoption on their own.

The journey of SMEX proved that while reputation is the true currency of technology, that reputation must be built through a balance of technical trust and visible, local effort. Their experience taught the project that deep research into journalist needs is only one half of the equation; without a simultaneous, aggressive outreach strategy to pull the community into the network, the infrastructure remains an empty vessel. This lesson emphasized the necessity of integrating local, physical spreading of the word alongside technical development to ensure that secure tools are not just reliable, but also inhabited.

Delo (Russia)

Delo operated under extreme legal and political pressure, resulting in a masterclass in high-stakes engineering within a shrinking civic space. Their strategy focused heavily on technical bridges and legal defense, knowing that the state was actively blocking external tools and pushing users toward monitored platforms. To counter this, they developed a Telegram-to-Mastodon bridge, which addressed the primary obstacle of decentralized technology: the fear of losing an existing audience. By allowing content to flow between platforms, they provided activists with a safe exit from surveillance-heavy apps without cutting them off from their followers. Their work demonstrated that in high-risk environments, trust and physical safety are far more important than a polished interface.

However, the project faced a significant turning point as the legal environment in Russia grew increasingly hostile, particularly with the designation of LGBTQ+ movements as extremist. This shift created immense financial and personal hurdles for the team, as members were forced to navigate a landscape where their very existence was criminalized. These external pressures led to a critical loss of human and financial capacity. While the project began with a strong foundation and meticulous planning, these escalating threats eventually made it impossible to sustain the initial momentum.

The experience of Delo serves as a profound lesson on the limits of technical resilience when faced with overwhelming risk. Their close collaboration with lawyers ensured that the project remained a tool for safety rather than a legal liability, but the ultimate takeaway is that digital tools cannot exist in a vacuum. The sustainability of decentralized infrastructure is directly tied to the physical and financial security of the people who maintain it. Despite the reduction in capacity toward the end of the pilot, their early success in building secure bridges remains a vital blueprint for how technology can be used to protect vulnerable communities under the most severe forms of state surveillance.

The following data provides a snapshot of the digital footprint created during the pilot phase. These numbers reflect the varying degrees of success in transitioning from technical setup to active community use. To ensure the success of these deployments, all partners were provided with comprehensive technical training and dedicated workshops on building effective outreach strategies. Furthermore, consistent technical support was available throughout the project to assist with troubleshooting and infrastructure maintenance.

Platform		**Colnodo**	**Redes**	**CITAD**	**SMEX**	**Delo**
Mastodon	**Num. of users**	19	30	318	0	0
	Num. of Posts	45	196	1,083	0	0
Element	**Num. of users**	22	35	*0*	0	0
	Num. of Private Rooms	20	42	*0*	0	0
Peertube	**Num. of uploads**	1	0	0	0	0

The quantitative results highlight three distinct models of decentralized adoption that emerged during the project. In Nigeria, CITAD achieved the most significant public facing growth, proving that when decentralized tech is paired with culturally adapted outreach, it can successfully function as a bustling community hub. This high volume of activity demonstrates a clear appetite for digital sovereignty when the infrastructure is made accessible at the local level.

While their social media engagement was high, the outreach for Element was significantly delayed due to persistent technical hurdles with email configurations at the start of the project. This long standing issue prevented the team from onboarding users to the chat platform as planned, illustrating how even a single technical bottleneck can stall the momentum of a broader engagement strategy.

In contrast, the data from Mexico and Colombia reveals a focus on quality of interaction and secure coordination. Redes successfully fostered a dedicated core of users with a high engagement to user ratio, indicating that their strategy created a space for regular, meaningful communication rather than passive consumption. Meanwhile, Colnodo's activity highlights a community using the platform specifically for sensitive coordination, as shown by the near one to one ratio of private rooms to users. This proves the value of decentralized tools as digital safe houses for high risk defenders.

Finally, the lack of user data for Lebanon and Russia serves as a critical lesson on the necessity of proactive community engagement. In these regions, the impact was hindered by a lack of effective on the ground outreach and a failure to implement the human bridge required to onboard users. While the technical infrastructure was made available, these zeros prove that technology alone cannot drive adoption. Without a properly executed outreach plan and the selection of partners capable of sustained community organizing, the infrastructure remains an empty vessel, regardless of the quality of the engineering or the intensity of the local political pressure.

Key Findings

When looking at these five diverse regions together, several striking patterns emerge that define the dComms experience. Across every context, trust in the local partner was an important factor for adoption, this proves that decentralized tools are not just technical products but social ones, relying entirely on the credibility of the people who deploy them.

The project revealed a clear divide between technical deployment and actual community appropriation. In Nigeria, Colombia, and Mexico, the innovations succeeded because the technical solutions—like solar-powered servers—were paired with deep, continuous, on-the-ground outreach. These partners demonstrated that when the technology addresses a survival need and is backed by physical community engagement, adoption follows.

In contrast, the experiences in Russia and Lebanon showed that even the most sophisticated technical bridges or stable infrastructures remain underutilized if the local environment prevents active outreach. These cases highlighted a critical strategic reality: while technical reliability is the baseline, it cannot compensate for a lack of local, physical spreading of the word.

Furthermore, the collective experience identified that the monopoly of commercial platforms is reinforced by powerful economic incentives. In Nigeria and Mexico, the project documented that Big Tech stays dominant because it functions as a digital marketplace and a source of income. In Colombia, for example, community members were interested in the autonomy of the tools but were hesitant to migrate because they needed to sell their local products, and the Mastodon platform did not yet have a large enough audience to support their livelihoods. Similarly, in Nigeria, influencers and young professionals were reluctant to leave mainstream apps where they have established revenue streams and global visibility.

These examples create a significant barrier for privacy-focused alternatives, proving that the final takeaway of dComms is that digital resilience is a dual-track process. A project must be as committed to high-effort community building and economic relevance as it is to rock-solid engineering. These five journeys prove that decentralized tools only move from a pilot to a living network when they are adapted to the unique physical, economic, and political realities of the communities they serve.

5) User Experience Assessment: Feedback on tool usability and accessibility

A recurring theme throughout the dComms was the struggle between making a tool safe and private, versus making it easy to use. For the diverse user base our partners serve—ranging from activists to rural community members—a tool that offers 100% security but requires a twenty-minute technical setup creates a barrier that most non-technical users won't cross. Over the course of the project, our partners dedicated months to identifying the specific friction points where the user journey often met a premature end.

I. The Onboarding Wall

The most significant hurdle occurred at the very first step of the process. Most participants are accustomed to the streamlined onboarding of big tech platforms, where entry requires little more than a phone number. In contrast, users in Nigeria and Colombia found the decentralized concept of choosing a server to be a major roadblock. The requirement to select a specific instance, such as social.nazlo.space, rather than simply joining Mastodon, created a cognitive load that stopped many users before an account was even created.

This was compounded by the email bottleneck, which emerged as the primary technical complaint across all partner regions. When automated email verification systems failed or were delayed, the user journey ended instantly, as there was no secondary path to account activation.

II. Hardware and Data Limitations

Usability is also dictated by the physical constraints of the hardware used in the field. Our users in Nigeria and Lebanon, for example, often rely on older smartphone models with limited storage and processing power. For these individuals, the Mastodon and Element applications frequently felt too heavy, leading to system crashes or significant device slowdowns.

Furthermore, in Mexico and Colombia, where mobile data is a precious and expensive commodity, users were highly sensitive to consumption rates. Unlike lightweight alternatives like Telegram, some Fediverse tools were perceived as data hungry, consuming monthly plans at a rate that felt unsustainable for the average user.

III. Interface and the Learning Curve

The interface design itself presented a steep learning curve, particularly regarding encryption. While the Matrix protocol provides industry-leading security, users found the

key management features—such as recovery phrases and the green shield verification—highly intimidating. Many participants lost access to their encrypted chats because they did not understand the necessity of saving security keys, with one user noting, "I just want to chat; I don't want to be a cryptographer."

Additionally, the lack of an active social circle Made it hard to keep users coming back; without the instant gratification of a pre-populated feed or the presence of established influencers found on X or Instagram, users felt less motivated to engage with a local Mastodon instance on a daily basis.

IV. Accessibility and Language Barriers

Language was also a challenge at times, many of the help menus and error messages were only available in English. For users in Russia or rural areas who don't speak English, seeing an error message they couldn't read made it feel like the tool wasn't for them. Because the apps weren't always easy to figure out, our partners had to spend a lot of time helping people individually. We found that for every ten new users, we needed about one "mentor" to guide them through their first week so they could get comfortable with the tool.

V. The "Safe Start" Hybrid Model and Final Verdict

Toward the conclusion of the project, a clear preference emerged for bundled, hybrid models. In Russia, the bridge functionality proved to be the most successful UX feature. Users appreciated the ability to remain within their familiar Telegram interface while their messages were securely routed to a Mastodon server. This magic button approach provided the security of dComms without sacrificing the smoothness of a mainstream app.

To better understand these challenges, the following section breaks down the user experience for each specific tool deployed during the project, based on direct feedback from users and community administrators.

Element (Matrix)

While there was high interest in Element for its secure communication, the registration process was described by many as very annoying and a major barrier to adoption. Users were often forced to start their registration in a mobile browser before they could even use the app, which was a long and multi step process that led many to give up. Once

active, the complexity of device synchronization and cross verification created significant confusion. Users frequently found that messages sent from a phone appeared as unverified on a browser, or vice versa. This complexity, combined with the fact that many users forgot their passwords or recovery keys, led to frequent data loss where all prior message history was deleted. For users with limited technical knowledge who rely solely on mobile phones, these hurdles made the tool feel inaccessible for daily use.

Mastodon

Mastodon was generally found to be easier to use than Element, but it faced significant hurdles regarding onboarding and cultural fit. A recurring issue was the manual entry of domain names; users often made typos when typing in the community server address or accidentally registered on the wrong external servers. This led to requests for a more simplified, one click entry to keep users within the community owned infrastructure. Furthermore, while the privacy features were appreciated, many users found the platform felt empty. Because the goal for many communities is broad reach and viral potential to promote events or local products, the lack of a pre populated social circle and the smaller scale of the local instances made it difficult for users to stay engaged long term.

PeerTube

The feedback on PeerTube was mixed, highlighting a gap between interest and daily habits. In some contexts, it was seen as an easy way to consume video without needing an account, but in others, the community did not find the tool attractive because they were not accustomed to producing or watching long form videos on a daily basis. Users tended to jump between different platforms rather than sticking with a dedicated video server. While the idea of a censorship resistant video space was respected, the lack of a consistent habit for long form content meant that PeerTube did not achieve the same level of active, daily engagement as the chat or social networking tools.

The final UX verdict is clear: to scale these tools effectively in the future, the security must become invisible. Users should not have to solve a technical puzzle to communicate; the goal is to reach a point where the most secure option is also the most effortless one.

6) Adaptive Strategy: The Pilot Extension (Fluffychat Testing)

The transition from Element to FluffyChat marks a strategic shift in the dComms project's approach to user-centric security. While Element provided the robust technical foundation required for decentralized communication, initial deployment metrics indicated that its interface was a significant barrier for non-technical users. To address this, we initiated a pilot extension focused on FluffyChat—a minimalist Matrix client designed to prioritize usability. This pivot was intended to lower the entry threshold for our partner communities while maintaining the core principles of the Fediverse: privacy, sovereignty, and resilience.

Early data from this extension confirms that a "less is more" approach directly correlates with higher adoption rates. Across the testing groups, the transition to a cleaner, more intuitive interface solved many of the UI-related frustrations documented previosuly. However, while the visual experience improved, the underlying technical infrastructure of the Fediverse—specifically the requirement for custom homeservers—remains the primary point of friction for new users.

- **Partner Case Study: Colnodo (Colombia)**

The implementation at Colnodo serves as a vital proof of concept for this adaptive strategy. Users responded exceptionally well to the simplified design, awarding the application a 5.0/5.0 for design clarity. The consensus among the community was that FluffyChat feels lighter and more intuitive, particularly for those accustomed to mainstream messaging apps.

Despite these gains, the first mile of the user journey remains a significant technical and psychological hurdle. The process received a low rating of 2.0/5.0, primarily because account creation cannot be completed natively within the FluffyChat application. Instead, users are forced into a fragmented workflow: they must first exit the app to register via a web browser at the specific domain before returning to the app to log in.

This requirement to switch between a browser and the mobile interface—compounded by the need to manually enter a long, custom homeserver address—confuses users who are accustomed to the seamless, one-click registration of centralized platforms. For many, this out-of-app registration felt like a major technical barrier, leading to longer onboarding times and a higher risk of user drop-off before the first message is even sent.

While the minimalist design was widely praised, the absence of natively integrated voice and video calling within the mobile application presented a challenge for professional workflows. Unlike mainstream tools where these features are built-in, FluffyChat requires users to initiate calls via external links (such as Jitsi). While this maintains the project's commitment to decentralized, open-source modularity, the transition from a chat interface to an external browser or app for a call created a fragmented user experience.

Technical hurdles also emerged during the testing phase, including server overloads during high-demand periods and a temporary disruption of access tokens following a Docker update.

- **Partner Case Study: REDES (Mexico)**

The implementation at REDES followed a highly disciplined, capacity building approach, prioritizing the removal of technical friction to protect the physical and digital autonomy of their users. Their strategy focused on moving beyond out of the box settings to create a localized onboarding ecosystem tailored for territorial defenders and journalists.

A major success in this phase was the internal growth of the technical workflow through containerized environments. This shift allowed the team to gain greater control over the infrastructure, specifically tweaking Synapse and its database to better meet the unique needs of their partner communities. By migrating to a more stable VPS, they reinforced the idea that for high stakes work, infrastructure reliability is a fundamental safety requirement.

To address the documented onboarding wall, REDES developed a custom registration portal that decoupled the sign up process from the main chat application. This dedicated interface significantly reduced the cognitive load on new users by providing a clearer path to account creation. Furthermore, they integrated mobile first utilities, such as direct app download prompts and a copy to clipboard button for server URLs, which led to a higher first use success rate as users moved from browser based registration to a native mobile experience.

The analysis of this deployment revealed a distinct behavioral trend: users showed high engagement in private groups and direct messaging, but almost zero interest in public rooms. This reinforces the role of these tools as secure digital hubs for coordination rather than public social spaces. Additionally, the feedback highlighted a cultural adoption hurdle regarding the sticker gap. Users desired the same ease of expression found in

commercial apps, proving that bridging this fun gap is essential for long term community retention.

Despite these gains, REDES identified persistent challenges regarding identity and data persistence. In alignment with their privacy values, they do not require email addresses for registration, which has made password recovery a manual and administrative burden. Furthermore, the complexity of encryption keys remains a critical vulnerability for users who only own one device, as losing that device could mean the permanent loss of organizational history. Ultimately, the REDES experience demonstrated that infrastructure stability and a mobile centric approach are the essential pillars for adoption in diverse, high impact environments.

- **Partner Case Study: CITAD (Nigeria)**

The implementation at CITAD provides a critical data set regarding high-density onboarding and the educational curve of decentralized tools. With over 100 new accounts created during the pilot, the CITAD experience reinforces that while the UI shift to FluffyChat is positive, the infrastructure gap remains the primary friction point.

Users expressed a strong appreciation for the application's minimalist design and robust security features, particularly the end-to-end encryption. The consensus among students and staff was that FluffyChat offers a professional and secure sovereign alternative to mainstream platforms. However, the deployment revealed that even a superior UI cannot fully compensate for a fragmented onboarding architecture.

The first mile of the user journey proved to be a significant hurdle. Similar to the findings in Colombia, the out-of-app registration requirement was the primary cause of user frustration. Because account creation cannot be completed natively within FluffyChat, users were forced into a fragmented workflow: exiting the app to register via a web portal before returning to log in. This loop, compounded by the complexity of the Matrix ID format (@username:matrix.citad.org.ng), made user discovery less intuitive compared to phone-number-based apps.

Technical hurdles were also prominent during the testing phase, specifically regarding server capacity. During mass sensitization sessions, the local Matrix homeserver reached rate-limiting thresholds, triggering “server busy" errors for multiple simultaneous registration attempts. In a pedagogical setting, these errors created immediate skepticism toward the tool's reliability and highlighted the need for server-side optimization to handle the burst registration phases typical of community workshops.

Despite these challenges, the CITAD community showed a high level of security trust. The willingness of participants to navigate the technical learning curve suggests that for activists and students in restrictive environments, the value of decentralized resilience often outweighs the initial inconvenience of the setup.

Conclusion

The pilot testing across Colnodo, REDES, and CITAD confirms that FluffyChat is currently the best-fit client for these communities. Its success is rooted in a user-first design philosophy; the easy, familiar, and simple interface successfully lowered the psychological barrier to entry that had previously hindered adoption with more complex tools. By prioritizing a clean visual experience and essential features, FluffyChat allowed users to feel immediate at-home comfort, which is reflected in the high design ratings across all regions.

However, the testing also highlighted that a polished UI cannot fully mask a fragmented onboarding process. The first-mile journey—specifically the need for out-of-app registration and the manual entry of complex homeserver addresses—remains the project's most significant point of friction. To bridge this gap between decentralized sovereignty and mainstream ease of use, future iterations should prioritize the integration of Single Sign-On (SSO) features. Implementing SSO would allow for a native, one-click onboarding experience, removing the need for external browser registration and ensuring that the first impression of the dComms suite is as seamless as the chat experience itself.

7) Technical Recommendations: Guidelines for future Fediverse deployments

This project gave the dComms technical team significant valuable insight, for both areas to improve, and things that worked well.

Starting with the good: The installation process was largely *not* a pain point for partners. Specifically the Bash install script was streamlined enough to go off without a hitch for partners that had low but not no experience with the Linux command line. One caveat is that several common configurations (like providing mail credentials for sending from the services) should be added to the install script, as manually editing the config files are where most admins got stuck or had trouble. The fewer steps that require manual intervention the better. To reiterate the point, this framework for installing dComms is a reasonable UX design for that kind of administrator. That said, our goal for dComms is for it to grow beyond its niche, and so future projects should target an even more accessible install process, to empower users without Linux command line experience to also install dComms.

Another point that caused users (and so admins) some headache is account management. The present dComms bundle contains up to 4 services, each with their own individual user databases and authentication flows. For users managing credentials for even two services is difficult, let alone 4.

Our recommendation is to centralized authentication using a single sign on provider like Keycloak, or Authentik. This will enable users to sign on once, and be granted access to all the services, bypassing the need for a registration token for Synapse (another major pain point, as the mobile clients don’t have great support for this registration flow).

8) Outreach Recommendations: Lessons learned on community engagement

The dComms project demonstrated that deploying technology is only half the battle. The most significant lessons learned were about how to effectively engage communities to move toward digital sovereignty. Based on the real world experiences of our partners, we recommend the following strategies for future outreach and engagement.

One of the most important lessons is the need to leverage pre-existing social habitats. We learned that communities do not easily form new networks purely for the sake of using a new technology. Successful engagement happened only when dComms tools were integrated into the social groups and networks that people already used for their daily lives. Future outreach should not ask users to leave their communities but should instead bring the Fediverse to the spaces where they already gather, such as local mutual aid groups, neighborhood associations, or activist collectives.

We must also shift from a crisis narrative to a focus on daily utility. Initially, some outreach focused on dComms as a backup plan for internet shutdowns. However, outreach must instead emphasize the daily benefits of community owned infrastructure, such as privacy from corporate surveillance and local content ownership. People must use the tools every day for them to be effective when a crisis actually occurs.

Another critical factor is addressing the data hunger barrier in our communication. Our experience in Mexico showed that high mobile data costs are a major deterrent. If people feel that using a private tool will cost them more money than using a corporate one, they will choose the corporate one. Clear communication about data usage is essential, and we must provide users with practical data saving tips. Future technical development must prioritize making these tools as light as the commercial apps.

The necessity of local mentorship cannot be overstated. Across all regions, from rural Colombia to urban Mexico, the biggest barrier to adoption was the technical setup. We found that without a human bridge, such as a local mentor to walk users through the first steps, most people abandoned the tools immediately. Outreach should focus on a train the trainer model. Instead of broad marketing, we should invest in local tech champions within each community who can provide hands on, face to face support for new users.

The importance of this human layer was clearly visible in Russia and Lebanon, where the project’s impact was hindered by a lack of effective outreach on the ground. We learned that failing to properly implement a localized outreach strategy causes adoption to stall, regardless of how well the technology performs. A successful deployment requires partners who are not only technically proficient but also deeply committed to and capable

of sustained community organizing. Without a partner who can effectively build a human bridge to the users, the transition to new digital spaces cannot take place.

Finally, we must prioritize cultural and linguistic adaptation. The technical language of the Fediverse can often feel like a barrier to entry. Partners like CITAD and Colnodo noted that the tools felt foreign because the interface and the outreach materials were not always adapted to local contexts. All outreach materials must be co created with local partners to replace technical jargon with conversational language that reflects the specific values and needs of each community, such as focusing on digital safe houses or community libraries.

We have learned that a successful migration from Big Tech cannot be forced through technical superiority alone; it must be nurtured through human connection.

For a decentralized ecosystem like dComms to truly thrive, our outreach and our software must be as decentralized as our mission. This means moving away from top-down tech delivery and instead rooting our efforts in local trust and user-centric design. We have seen that the most resilient networks are those that are driven by local needs and managed by the people who use them. Whether in the rural villages or the activist circles, the technology only became relevant when it was both useful and usable.

Ultimately, the sustainability of dComms depends on a long-term commitment to both human interaction and technical simplicity. By supporting the social structures that surround the technology and making the software more approachable, we ensure that digital sovereignty is not a luxury for the few, but a practical, daily reality for the many. True independence from Big Tech is found in the strength of the communities we build and the ease with which they can stay connected.