SplinterCon

Challenging Digital Colonialism

2026
ONLINE

eQualitie

SplinterCon is an international and interdisciplinary conference that focuses specifically on internet fragmentation and its consequences on contemporary societies and online liberties. The inaugural event was launched by eQualitie in Montreal, December 2023. Since then, we've hosted SplinterCon to Brussels, Estoril, Berlin, Taipei, Paris, and, finally, online in May 2026. These gatherings assembled hundreds of creative minds from communities encompassing network researchers, technology entrepreneurs, network engineers and software developers, user experience designers, media and internet freedom advocates, in order to:

- Analyze the practices and impacts of network isolation and shutdowns;
- Evaluate existing and future technology solutions for communicating with and within sovereign networks;
- Invest in practical and user-oriented solutions for connectivity and content distribution across digital barriers.

SplinterCon is normally held under Chatham House rule, and we have sought explicit permission from presenters to share their materials for post-conference reporting. This collation presents highlights from three events and summarizes the 'state of the splinternet' as a point of reflection and in order to strategize from hereon.

Acknowledgments

We are deeply grateful to the SplinterCon speakers, whose support have shaped this project from the very beginning.

Dmitri Vitaliev
Technology Director,
eQualitie

Ksenia Yermoshina
Researcher,
eQualitie, The Center for Internet and Society, CNRS

Alejandro Mayoral Baños
Co-Executive Director,
AccessNow

Arzu Geybulla
Co-Executive Director,
AccessNow

Felicia Anthonio
#KeepItOn Campaign Manager, AccessNow

Anna Romandash
Media Freedom Ambassador of Ukraine

Mable Amuron
Researcher, Thraets Foundation, Uganda

Charlotte Escorne
PhD Candidate, IFG Lab,
Paris 8 University

Alena Epifanova
Research Fellow, DGAP,
Berlin

Marla Rivera
Founder & Director,
InterSecLab

J. Alex Dalessio
Executive Director,
eQualitie

Mahsa Alimardani
Associate Director,
Technology Threats,
WITNESS

Farzaneh Badiei
Founder, Digital Medusa

Patryk Pawlak
Project Director, Global Initiative on the Future of the Internet

Nils Berglund
Project Lead, Global Initiative on the Future of the Internet

Kehinde Adegboyega
Executive Director, HRJN Nigeria

Joana Mhone
Patch & Vulnerability Specialist, TNM Malawi

Daouda Diagne
Director, Computech Institute, Dakar

Vinicius Fortuna
Creator, Outline VPN

Wisdom Nji
Founder & Lead Engineer, Afkanerd

Bobby

Providence Baraka
Founder & Program Associate, Bingwa Civic Tech Lab, DRC

Jeremy
Deflect Lead, eQualitie

Hammer
Founder & Director, Project Ainita

Contents

Introduction

The 2026 edition of SplinterCon was not supposed to happen this way. It was conceived as an in-person gathering in Lusaka, Zambia, co-located with RightsCon, the flagship global digital-rights convening organized by Access Now. Days before it was due to open, RightsCon was cancelled: a foreign power, exercising influence over the host government, made it impossible to hold a meeting of digital-rights defenders, researchers, and technologists on Zambian soil. The SplinterCon that resulted (convened online on May 5, 2026) thus opened under conditions that were themselves a demonstration of its subject: information control had reached across borders to silence a community before it could assemble.

The response was immediate. Speakers and organizers pivoted to a virtual format within days. What might have drawn eighty people to a banquet hall in Lusaka instead convened more than three hundred registered participants from across the globe. As one of the co-organizers put it in his opening remarks, gathering in larger numbers when somebody tries to shut a community down is exactly how that community answers censorship. The cancellation was, in the words of eQualitie founder and technical director Dmitri Vitaliev, a reminder that the splinternet is already here: over two hundred million people now live inside networks designed and operated as national internets, and the Russian and Iranian models, should they endure, are likely to be copied elsewhere.

This edition placed the African continent at its center. Africa, in the framing of SplinterCon lead researcher Ksenia Ermoshina, acts as a prism that makes visible the intertwined logics that make splinternets possible: authoritarian regulation that treats connectivity as something a government may switch off at will; fragile and dependent network topologies whose routing paths run through foreign hands; the economic and political interests of the “global north” in shaping African cyberspace; and surveillance and censorship sold as a marketplace product, exported from one region and installed in another.

The history of the African internet is marked by colonization at every layer, from the physical cable to content and culture — and those dynamics persist even where formal political independence was won generations ago, because infrastructure, unlike flags, does not change hands at independence ceremonies.

The report follows the architecture of the day. Chapter 1 examines the lived experience and political economy of shutdowns in Africa. Chapter 2 maps infrastructural colonialism — the foreign vendors and policymakers whose investments in African networks do not always serve African civil society. Chapter 3 turns to the technical solutions, emerging technologies, and forward-looking tools that the internet-freedom community is building to keep people connected within and across splintered networks.

Chapter 1

Shutdowns in Africa: experiences and explanations

Shutdowns in Africa: experiences and explanations

If the *splinternet* is the methodical construction of digital borders, the internet shutdown is its blunt, immediate instrument, and Africa has been living with it longer than most. The continent has functioned, in effect, as a laboratory of shutdowns: a place where the disconnection of whole populations has become routine enough to reveal both the mechanics of the practice and the human cost it imposes. What distinguishes the African experience is that these shutdowns are often local and targeted rather than the wholesale national isolation seen in Iran or Russia, yet their cumulative effect is no less severe.

A decade of documenting shutdowns

The chapter's framing came from the keynote by **Felicia Anthonio**, who leads the *#KeepItOn* campaign at Access Now. The first deliberate shutdown she traced to 2006, when Guinea's president, facing strikes and protests, ordered the world's first, citing national security. Iran reused the tactic against the Green Movement in 2009; Egypt took it further in 2011 with a near-total blackout of internet, voice, and SMS. By 2016, Access Now and partners launched *#KeepItOn* to coordinate the pushback. The coalition has since grown into a global network of more than 366 organizations across 105 countries.

2,102

shutdowns documented worldwide, 2016–2025, across 100+ countries

313

shutdowns in 2025 across 52 countries — a record high, up from 304 in 2024

125

shutdowns in 2025 tied directly to conflict, across 14 countries

Anthonio's central observation was that what began as an experimental authoritarian tactic is now a primary tool used by democratic and authoritarian governments alike. In 2025, she reported, not a single day passed without the internet being shut down the internet somewhere in the world. The justifications have barely changed in two decades — national security, public order, curbing misinformation, preventing exam cheating — but the real triggers, she argued, are consistent: protests, contested elections, and the desire to control a narrative or conceal abuses. Shutdowns, in her phrase, do not happen without a reason;

there is always something on the ground a government is trying to hide.

The durations are punishing. Anthonio cited Iran's population being deliberately cut off for more than sixty days at the time of speaking; Ethiopia's Tigray region disconnected for over two years amid conflict; and an ongoing shutdown on the small island of Annobón, in Equatorial Guinea, running since 2024. Increasingly, she warned, governments target the alternative connectivity that people fall back on — confiscating satellite terminals, threatening users with arrest, or, as in Uganda before its elections, prevailing on Starlink to restrict service even where the company holds no operating licence. As VPNs and then satellite links are picked off, the case for more resilient tooling grows.

Hybrid warfare and the cross-border shutdown

A recurring theme was that shutdowns increasingly function as instruments of hybrid warfare, reaching across national borders. Anthonio's data recorded eighteen instances of cross-border shutdowns in seven countries in a single year: Israel responsible for disruptions in Palestine, Russia targeting ICT infrastructure in Ukraine, Thailand affecting Cambodia and Myanmar, China affecting Myanmar, and a Cameroonian disruption spilling into the Central African Republic. Measuring responsibility, she explained, sometimes rests on direct evidence such as airstrikes on telecommunications infrastructure, and sometimes on indirect leverage. In Palestine, for instance, Israel's control over fuel supplies eventually degrades the ICT infrastructure that depends on it. This work depends on joint remote and in-country measurement, corroborating a drop in traffic against events on the ground.

The Ukrainian journalist **Anna Romandash**, moderating the infrastructural-colonialism panel later in the day, situated this in lived reality. Since the start of Russia's aggression, she noted, there have been repeated attempts to reroute internet traffic in occupied Ukrainian territories through Russian networks, to replace Ukrainian providers, to impose censorship, and to isolate people from the global internet. Control over infrastructure (e.g. telecom networks, routing, energy grids, platforms) becomes a weapon, and fragmentation can be imposed deliberately as a strategy of domination. Sovereignty in the twenty-first century, she argued, is inseparable from digital infrastructure: a democracy cannot be protected if its information space is open to external control.

Who pays: differentiated harm

Shutdowns do not fall evenly. Anthonio stressed that their impact depends on what a person relies on the internet for, and that vulnerable groups are hit hardest. When Afghanistan was disconnected, women — already barred from education — lost the online channels through which they accessed learning and reproductive-health information. In conflict, the loss of connectivity means losing the ability to learn which routes are safe, to reach humanitarian aid, or to document abuses; it becomes, quite literally, a matter of life and death. To preserve these accounts, Access Now maintains a Shutdown Impact Stories project and the STOP (Shutdown Tracker Optimization Project) database, open since 2016.

Joana Mhone, a patch-and-vulnerability specialist from Malawi attending her first SplinterCon, sharpened the point into a warning about the tools people reach for in panic. Drawing on Access Now's own dashboard, she traced a decade of African shutdowns rising again after a brief dip, reaching some thirty in 2025. When networks are throttled or services blocked, she explained, people scramble for circumvention tools shared through unverified links, USB sticks, and WhatsApp groups, most often, free VPNs. The hidden cost is steep: by her figures, roughly 88 percent of free VPNs leak user data and around 71 percent share personal data with third parties, with some routing other users' traffic through an unwitting person's device, exposing them to liability for a stranger's activity. The tool meant to protect becomes a mechanism of exposure, and harm accumulates silently.

Three factors, Mhone argued, make this especially acute in Africa: a knowledge gap, in which cybersecurity is wrongly seen as the concern of professionals rather than ordinary users; peer-based spread, in which a malicious app travels by word of mouth during a crisis; and financial constraint. A paid VPN costing twenty dollars is trivial in the West, but in her country twenty dollars is a month's commuting budget. Her prescription was to treat safety as infrastructure: free, vetted circumvention tools provided as essential community infrastructure, like clean water, with knowledge built before a crisis rather than during it, through frameworks localized to people's literacy and means.

Accountability in the dark

The final movement of the chapter concerned accountability — how, when the lights go out, abuses can still be documented and someone held to answer. **Nils Berglund** of the European University Institute argued that accountability is, before it is a political problem, an epistemic one: governments are skilled at making digital-governance

commitments and poor at being held to them, and there is far more data on connectivity and infrastructure than on human rights. What can be measured shapes what can be evaluated, producing an accountability deficit in precisely the places where independent data is hardest to collect. He described an “accountability stack” in which any broken link — a data gap, an institutional gap, an enforcement gap — severs the chain from a shutdown event to a legal remedy.

Yet the chain can be closed. Berglund cited Kenya in 2024, where a coalition of civil-society organizations used network-measurement data from OONI, Cloudflare, and IODA to document election-period shutdowns and persuaded the high court to issue interim orders — a direct line from measurement tool to legal remedy. He pointed to regional initiatives such as Paradigm Initiative’s Londa index and Research ICT Africa’s After Access surveys, and urged the community to feed local and regional evidence into the forthcoming UN review of ICT measurement methodologies, due in 2027, where the indicators and baselines that will count as legitimate are being decided now.

Kehinde Adegboyega, executive director of the Human Rights Journalists Network in Nigeria, made the case concrete through the 2020 Lekki toll-gate shooting, where the military first fired on peaceful protesters and then denied being present, a denial undone by preserved live-stream footage. His organization built what he called a pipeline of truth: capture by grassroots activists, forensic verification in a lab, and secure archiving, with metadata preserved so that material can be verified and geolocated and distinguished from AI-generated fabrication even when uploaded long after the network returns. Resilience, he argued, requires the right toolkit — offline documentation, mesh networking, and the understanding that encryption is a survival mechanism, not a luxury.

Daouda Diagne, director of the Computek Institute in Dakar, closed the panel with the Senegalese case and a transition toward the question of sovereignty. Senegal is highly connected — extensive fiber, five ISPs, high mobile penetration, with more than 96 percent of users reaching the internet by phone — yet a single government notice can splinter it, as it did in 2021 and twice in 2023, each time for political reasons. A survey he cited found that more than half the population relies on digital tools for daily life, that business losses ran to roughly seven million CFA per business during shutdowns, that 31 percent of users could no longer communicate with their families, and that a majority reported a resulting loss of trust in democratic institutions. His community’s answer has been to build, in advance, a network trained in measurement tools

and circumvention and engaged in advocacy with authorities: preparation rather than reaction. But he left a paradox that leads directly into the next chapter: how can a country claim digital sovereignty when it depends on foreign technologies, and when the same sovereignty rhetoric gives its government the legal power to splinter the network at will?

Chapter 2

Unveiling infrastructural colonialism

Unveiling infrastructural colonialism

The shutdowns of Chapter 1 have an underlying logic that reaches beyond the local. Information control is also a business and a means of projecting influence, and the African digital economy and internet topology are being shaped — and in places torn apart — by foreign investors whose interests do not always align with those of African civil society. The question to ask of any given investment is who sets the rules, who holds the data, and who can switch the system off. This chapter examines two cases through which those questions come into focus: Russian influence, and the competition of Chinese and American capital across the Gulf of Guinea.

Setting the scene: the splinternet and African elections

Mable Amuron, a research lead at Thraets working on AI, disinformation, and digital information ecosystems, opened the panel by establishing the stakes. Africa is digitizing fast: by her figures some 38 percent of Africans use the internet, 89 percent of them solely via mobile phones, with a sharp urban-rural divide. There are roughly 646 million users today, projected to reach 1.1 billion by 2029. The architecture chosen now, she argued, will determine the architecture of the continent's democracy, and digital sovereignty is a double-edged sword. Data localization, digital ID, and independent internet exchange points can protect citizens and lower costs; the same infrastructure can enable mass surveillance, opposition tracking, and shutdowns that become trivially easy once national choke points are controlled.

She traced how this plays out around elections, the moment when connectivity control becomes a political instrument. Uganda's trajectory ran from blocking social media in 2016, to a full shutdown in 2021, to a shutdown that also severed mobile money in 2026. Tanzania saw a nationwide outage on election day under cover of which, by her account, large numbers were killed and thousands of opposition supporters arrested. Nigeria in 2023 offered a subtler failure: a promised real-time results-transparency system went offline for hours on election night, with a substantial share of polling-unit results missing from the portal at the close, while fake result sheets circulated on WhatsApp — a platform that is, as she noted, opaque to fact-checkers and poorly served by content moderation in African languages such as Amharic, Xhosa, and Tigrinya. Her recommendations ranged from

human-rights benchmarking of sovereignty policies to AU- and ECOWAS-level frameworks prohibiting election-period shutdowns, and open-source monitoring of internet-exchange-point ownership.

Negotiating sovereignty: Chinese and American infrastructure in the Gulf of Guinea

Charlotte Escorne, a doctoral researcher at the French Institute of Geopolitics (Paris 8) studying the rollout of 5G in West Africa, used maps from her fieldwork to dismantle a common misconception: that African digital infrastructure is simply either Chinese or American. The reality, she showed, is more tangled. The mobile-equipment market is shared among five major vendors (Ericsson and Nokia (European), ZTE and Huawei (Chinese), and Samsung (Korean)) while submarine cables are typically built and run by consortia of telecom operators, alongside some American and Chinese players. African operators source equipment from all of these at once.

Two dynamics, she argued, are changing the sector. Under China's Digital Silk Road, Huawei and other Chinese actors increasingly offer turnkey "Smart [country]" projects — Smart Senegal and similar programs in Nigeria, Ethiopia, and South Africa — combining fiber with digital services for education, health, and urban management, but also, potentially, expanded population monitoring of the kind associated with "safe city" systems. Separately, major content providers such as Google and Meta are now investing directly in physical infrastructure. The central question becomes what these players mean for internet access and digital sovereignty.

Her case study was a March 2024 submarine earthquake off Côte d'Ivoire that damaged four of five cables on that route and disrupted connectivity across eighteen African countries — a vivid illustration of the lack of resilience in network infrastructure. She made two analytical points. First, dependence is shaped by the economic interests of whoever deploys and operates the networks, not a simple US-China divide. Second, new partnerships and technologies offer real opportunities to strengthen African agency, but with limits. Senegal and Côte d'Ivoire function as regional hubs not merely because they reach submarine cables (so do Ghana and Nigeria) but because they have dense terrestrial networks and cross-border interconnections, a configuration owed in large part to Orange's strategy of interconnecting the markets it serves. Chinese involvement in the region's submarine cables is in fact relatively limited — a single Chinese-built cable runs

from Dakar to Cabo Verde, and even that belongs to and is used by the Senegalese government. Zoom out to the continental scale, however, and the picture shifts: Huawei has deployed a significant volume of terrestrial infrastructure across Africa, closely aligned with the Digital Silk Road's diplomatic and economic engagement. Newer entrants such as Starlink complicate matters further, offering connectivity that can bypass local regulation — an advantage for users, but also a source of unequal competition for local operators and, in places such as Mali, a potential security concern. Her conclusion echoed the panel's refrain: digital sovereignty in Africa cannot be reduced to a binary contest between Washington and Beijing. It emerges from a complex interplay of global corporations, regional operators, and state actors, and governments are not passive, increasingly using infrastructure itself as a tool of control, as Senegal's own shutdowns during the protests of 2020 and 2024 attest. The challenge is not who builds the network, but who controls it and under what conditions.

Exporting the sovereign internet: the Russian model

Alena Epifanova, a research fellow at the German Council on Foreign Relations, presented early findings from a research project on Russia's export of its sovereign-internet model to African countries through platforms, infrastructure, contracts, and the strategic use of sovereignty rhetoric. She began with the model itself. Since 2019, Russia has built out a system of control grounded in its sovereign-internet law and in TSPU — deep-packet-inspection boxes installed directly in ISP networks that let the state filter, throttle, or block content at will. Alongside filtering sits SORM, a legal backdoor built into telecom networks granting the security services near-total access to transmitted information without the knowledge of users or providers. A third layer, platform substitution, compels companies handling Russian citizens' data to store it on Russian soil and surrender it on demand — a requirement domestic firms such as Yandex and VK comply with. The trajectory, she summarized, runs from blacklists in 2012 to network-level filtering in 2019 to the rollout of whitelists that leave only state-approved content reachable: surveillance and censorship by default.

This is the model Russia is now marketing abroad, and Africa figures prominently in its agenda. Epifanova traced three channels. The first is commercial platforms, exemplified by Yango — spun out of Yandex in 2024 and nominally headquartered in Dubai — which operates in more than a dozen African countries and is the ride-hailing market leader in Senegal, Côte d'Ivoire, and Zambia, while also offering food delivery,

logistics, lending, and fintech. The concern is data: investigative reporting has found no physical or logical separation between Yandex's domestic and international databases, meaning Yango trip origins, destinations, financial data, and communications flow into servers in Russia, where a 2023 law grants the FSB round-the-clock access. The Norwegian data-protection authority concluded that Russian authorities could potentially monitor Yango customers' movements; the Netherlands opened an investigation. No comparable regulatory scrutiny, she noted, has come from an African authority.

The second channel is surveillance infrastructure. The company Protei supplies SORM-compatible systems and deep-packet-inspection technology to telecom operators across several regions, including documented African deployments — a state operator in the Comoros installing DPI that appears to replicate Russia's surveillance architecture inside a national telecom, with projects reported in Nigeria and customers listed in Kenya and Tunisia. Protei's market-entry strategy, she observed, is to enter first as a traffic-management solution and then expand the product suite from within. The third channel is public diplomacy and education: a Higher School of Economics e-governance program running since 2021 and aimed explicitly at Africa, and a declaration on international information security adopted at the second Russia-Africa summit that calls for jointly opposing neocolonialism while affirming each state's sovereign right to regulate its national segment of the network. In practice, she argued, that framing invites African partners to adopt a governance model that carries surveillance and censorship as standard features.

Toward digital sovereignty as autonomy

The thread running through both cases is that "digital sovereignty" is a contested word. As Daouda Diagne had argued in the previous session, in Senegal it is often deployed as a populist slogan, and it can mean either independence from foreign technology or simply the government's own ability to splinter the network. The panelists' shared conclusion pointed toward a more constructive reading: sovereignty understood as autonomy — the capacity of African states and communities to build and govern their own infrastructure in the interests of their citizens, rather than either depending on foreign systems they cannot control or asserting a sovereignty that mainly empowers the state to disconnect its own people. That reframing (from sovereignty-as-isolation to sovereignty-as-self-determination) does not resolve the tension so much as relocate it: to the harder question of how communities build the infrastructure they need when the economics, the routing paths, and the regulatory frameworks all conspire against them.

Chapter 3

Technical solutions for splintered networks

Technical solutions for splintered networks

If Africa is a laboratory of fragmentation, it is also a blueprint, and so is Iran, where the dynamics are similar and where solutions developed under pressure may prove applicable elsewhere. The second half of SplinterCon turned deliberately forward, to the tools and infrastructures that can help communities stay connected within and across splintered networks. As Dmitri Vitaliev framed it, SplinterCon does not treat circumvention alone as the answer. The promise of digital technology is helping people determine their own pathway online: staying connected with each other in whatever network is available, through decentralized protocols, accessible wireless technologies, and rediscovered methods of routing, obfuscation, and content delivery. Several of the projects below are recipients of eQualitie's Breakout Program, which has awarded around half a million dollars in grants for practical, decentralized resilience work.

Open the skies: the potential and limits of Direct-to-Cell

A fireside chat with **Alex Dalessio**, **Mahsa Alimardani** (Witness; Oxford Internet Institute), and **Farzaneh Badiei** (Digital Medusa) took as its starting point the near-total shutdowns in Iran on January 8 and February 28, 2026, when at one point only some 1.4 percent of the internet was functioning. Badiei described an internet that had never been fully restored after January — nearly three months of shutdown during which none of the usual VPNs and circumvention tools reliably worked, and during which she had been unable to speak with her 87-year-old father. What had emerged in its place she called an "internet apartheid": a tiered, sectoral system granting expensive access through professional associations to the regime's supporters while leaving the population disconnected.

Against that backdrop, Alimardani explained the premise of the Direct-to-Cell campaign she helped initiate: satellite internet is internet. During the January blackout, when nothing else worked, a small window of connectivity was enabled through Starlink terminals — a drop in the bucket of perhaps fifty thousand devices, accessible only to those who could afford a thousand to two thousand US dollars to buy a smuggled receiver at great risk. The campaign's question was how to make that drop scale. Direct-to-Cell — connecting ordinary handsets to satellites without a ground terminal — exists today only in a basic, first-

generation form that still depends on cooperation with local carriers and nationally licensed frequencies. The opportunity lies in the second generation, expected within a few years, whose larger satellites work through spectrum ranges not governed at the national level.

The crux, Alimardani stressed, is that the regulations are being written now, in forums such as the International Telecommunications Union, ahead of the World Radiocommunication Conference in Shanghai in 2027 — and civil society has little seat at that table while states including Iran, China, and Russia are very much present. Badiei made the governance argument: digital sovereignty is invoked by democratic and undemocratic states alike to shield repression, as Iran did when it petitioned the ITU's Radio Regulations Board to have satellite terminals shut down even as it was killing protesters in the streets. If we truly believe in free global access, satellite internet is the one layer of infrastructure over which states should not be able to impose control, and the community needs a global-governance mechanism for it in which civil society can participate. The campaign is careful about scope: not everyone connecting by satellite, but satellite as a vital dimension of a still-terrestrial internet, governed by humanitarian protocols that could be triggered in defined crises. Alimardani's closing point answered the skeptic who asks why a long-term regulatory fight matters during an active shutdown: because the technology is emerging and the rules are being set regardless, and if civil society treats this as a low priority, others who consider it a high priority will shape it for years to come.

From gourmet tools to building blocks: scaling resilience

Vinicius Fortuna, who leads the Outline project, used his keynote to diagnose a structural weakness in the circumvention ecosystem and propose a remedy. Censors are moving faster and coordinating across borders: censorship is now sold as a product, deployed regionally. And yet the tool-building community keeps reinventing the wheel, producing monolithic "gourmet" tools that share almost nothing with one another. He walked through the lineage: plain proxies blocked by China; Shadowsocks disguising proxy traffic as random bytes; Trojan reskinning the same approach over standard TLS to blend in; V2Ray composing protocols but only within its own non-reusable platform, forcing forks whenever someone wanted to add something new. The names, he argued, hide what actually matters: the property that defeated the censor was usually a single layer (TLS, or WebSocket-over-TLS that lets a service hide behind a CDN) not the branded tool as a whole.

His proposal was a shared taxonomy of capabilities that lets builders decompose tools and recombine them like Lego. On the data plane he defined four: resolve (turning a name into a usable address, defeating DNS-based blocking through encrypted DNS); shape (altering traffic unilaterally from the client, with no server cooperation, to defeat SNI- and content-based blocking by splitting packets or reordering them); carry (the transport that actually moves the bytes — the layer the censor sees); and relay (the proxy itself, which can use a standard protocol such as SOCKS5 while the carry layer underneath is swapped freely). On the control plane he added strategy selection, measurement, and easy integration. The lesson for funders and builders is to stop turning protocol names into requirements and start asking what capability is actually needed.

The payoff is reuse. Fortuna noted that the Outline SDK now has over thirty million users across many apps, and that designing for reusability — documented APIs, permissive licensing, composable, single-responsibility components — shrinks the time from a new idea to real-world impact from years to weeks. He cited the Amnezia team adding support for its censorship-resistant protocol to a Russian news app through an Outline adapter, without any gatekeeping from the Outline team. To anchor the practice, he announced an "Awesome Outline" community registry organized by the new taxonomy. Why it matters for Africa, he closed, is that regional blocking can scale quickly, and a reusable, recomposable toolkit lets defenders adapt to local contexts and cut cost and maintenance by proxying only what truly needs proxying.

Understanding the censor to defeat it: Geneva on Deflect

Jeremy presented a new partnership between eQualitie's Deflect service and Geneva, the genetic-evasion tool developed by Professor Dave Levin's group at the University of Maryland. Deflect is a DDoS-protection and web-security service founded in 2011 that now protects roughly a thousand websites, sees on the order of fifty million daily HTTP hits, and — critically — finds that twenty to twenty-five percent of the sites it protects face censorship, mostly with their domains blocked in Russia and, in some recently discovered cases, their IPs outright blocked.

The idea is to shift the burden of evading censorship from the user to the website. Rather than asking every reader to install a VPN, the server side — or the CDN acting as middleman — takes on part of the work. Geneva ("genetic evasion," not the city) uses a genetic algorithm to evolve strategies against a given censor: series of instructions that manipulate

the packet stream on the server side to confuse the censor's middlebox. It works because middleboxes, facing enormous traffic volumes with finite resources, take shortcuts when they inspect packets — and those shortcuts are bugs Geneva can exploit.

The four manipulations it uses on TCP traffic are duplicate, fragment, tamper, and drop. In one example Jeremy walked through, when the server is about to send a SYN-ACK, Geneva replaces it with two tampered packets — an RST followed by a SYN — so that the censor's middlebox believes the connection has been reset and a new one started, desynchronizing its per-connection state from the client's real state, while the genuine client TCP stack handles the malformed sequence without trouble. The censorship fails; the connection goes through.

The work, Jeremy noted, is still at proof-of-concept stage and not yet in production. The roadmap for 2026 into 2027 involves making the Geneva engine production-ready for large traffic volumes — refactoring the Python proof-of-concept and possibly replacing iptables NFQUEUE with eBPF for efficiency — training strategies inside Russia, since censorship shifts and a strategy that works today may fail tomorrow, and adding IPv6 support, which can yield surprising results because censors often focus on IPv4.

Off the grid: responses to shutdowns and emergencies

The final cluster of projects addressed the hardest case — keeping people connected, at least locally, when there is no internet at all. Two were recipients of the current Breakout Program round.

Shortmesh — messaging bridges as infrastructure

Wisdom Nji, founder and lead engineer at Afnerd, presented Shortmesh, an open-source API built to integrate with Matrix bridges, which connect the Matrix protocol to platforms such as Signal, WhatsApp, and Slack. Shortmesh comprises a Matrix client, an interface API exposing those bridges over REST so developers can integrate quickly, and Shortmesh OT, a one-time-password generator that delivers codes through any bridged platform. It was built to solve a concrete problem for free and open-source projects: the cost of phone-number verification through commercial services such as Twilio. The tool offers a self-hostable alternative, a "sign in with Signal/WhatsApp" widget, and bidirectional communication that the team is folding into its own SMS Without Borders project to reduce SMS bandwidth and, ultimately, bring encrypted bidirectional communication over SMS to online platforms.

CommunityNet — an alert that reached eleven thousand households without the internet

Bobby (presenting by avatar for security reasons) described a multi-layer early-warning system built for a community living under a total communication blackout and repeated airstrikes — by his account, targeted 150 times in a single year — in a civil-conflict setting with no single authority to rely on. Traditional alerts such as bells, shouting, and drums do not scale. The system builds on an existing local fiber backbone as an intranet rather than an internet, and works because the community is a mobile-first generation with phones in hand. Two deliberately simple changes — packaging existing open-source tools together, and incentivizing users to log in weekly — let a single dashboard push an early warning to thousands of households at the click of a button.

The Breakout grant let the team cut app-installation time and, more importantly, raise notification delivery from about twenty percent of registered phones to sixty percent of active users — a roughly three-hundred-percent improvement — by solving the problem of cheap Android phones killing the app. A hardware layer adds sirens and LEDs driven by a local coordinator application on the existing solar-powered network. Because a fiber backbone is vulnerable to fire, wind, or landslide, the next stage is a wireless system using LoRa or HaLow connectivity, alongside efforts to make the community app useful day-to-day with weather and news so that people are familiar with it before a disaster strikes.

Raspberry Pi gateways — resilient access under ISP interference

Providence Baraka, founder and program associate at the Binwa Civic Tech Lab in the Democratic Republic of Congo, presented an approach to internet freedom under ISP-level interference, set against the 2025 shutdown in Goma ordered amid war. Where connectivity is predominantly mobile 3G and 4G, censorship is implemented at the ISP level through DNS manipulation, throttling, and deep packet inspection — and even standard WireGuard handshakes have detectable patterns that let an ISP block the server's IP. Commercial VPNs, he warned, are also black boxes that may sell data or comply with warrants.

His answer pairs minimalist hardware with a carefully considered software stack: a Raspberry Pi, battery- or power-bank-powered, creates a local access point and connects WireGuard clients to an external VPS for encryption, shipped with scripts so that non-specialists can bring more users online. Key design considerations include per-user

keys that can be revoked from the VPS if a device is seized, minimizing stored data to reduce forensic risk during inspections, DNS-over-TLS via Unbound to prevent ISP-level DNS poisoning, and unattended security upgrades. Recognizing that circumvention is not enough, he closed by pointing to offline, censorship-resistant peer-to-peer messaging — such as Briar, which connects over Bluetooth, Wi-Fi, or Tor — so that communities can keep communicating even when there is nothing to circumvent to.

Conclusion

The net will be decentralized...

Conclusion: the net will be decentralized...

SplinterCon Online began with an act of fragmentation — the cancellation that scattered a planned gathering and forced it onto the very networks whose fragility it had assembled to discuss. And it answered that act by gathering anyway, in larger numbers, online. That symmetry is the report's through-line. The cancellation of RightsCon was a demonstration of transnational repression; the shutdowns documented across Africa are a market and a method that travels; and the dependencies mapped across the Gulf of Guinea and exported from Moscow are the raw material of control. Africa, as a prism, made all of this visible at once.

Yet the day's deeper argument was that visibility is not despair. Across every chapter, the people closest to the harm were also the people building the answers — the Malawian engineer reframing safety as community infrastructure, the Nigerian journalists assembling a pipeline of truth, the Senegalese trainers preparing their networks before the next shutdown rather than after it, the Iranian advocates fighting for satellite internet as a human right in rooms where their governments hold the microphone, and the toolmakers from Dakar to Maryland to the DRC composing resilient connectivity out of reusable parts, off-grid sirens, and Raspberry Pi's.

Two lessons persist across all three chapters, neither as tidy as this report makes them sound. Technical solutions are most likely to hold when they are hybrid, several protocols and channels rather than a silver bullet, and built on shared components that others can adapt without starting over. But the deeper lesson resists being technical at all: every durable solution here depended on a community of practitioners in genuine contact with the people actually inside fragmented networks, close enough to iterate from the real conditions rather than from a model of them. That, in the end, is exactly the capacity the cancellation tried and failed to break.

eQualitie has been developing a new generation of circumvention and resilience technologies — decentralized protocols, distributed routing and storage, wireless and broadcast services, and countrywide fediverse and datacasting efforts that rebuild important content inside isolated networks. But the through-line of SplinterCon Online is that no single tool, and no single organization, gets ready for the splinternets alone.

Through the SplinterCon series we are building a network of human expertise and a shared pool of skill and knowledge to support digital communication and connectivity for the years to come. The net will be decentralized — and so, of necessity, must be the community that keeps it open.

This report was produced by eQualitie based on the proceedings of SplinterCon Online, May 5, 2026. Claude AI Opus 4.8 was used for text formatting and language polishing. For recordings, related research, and ways to get involved, visit splintercon.net.

splintercon.net/community

SPLINTERCON.NET

eQualitie