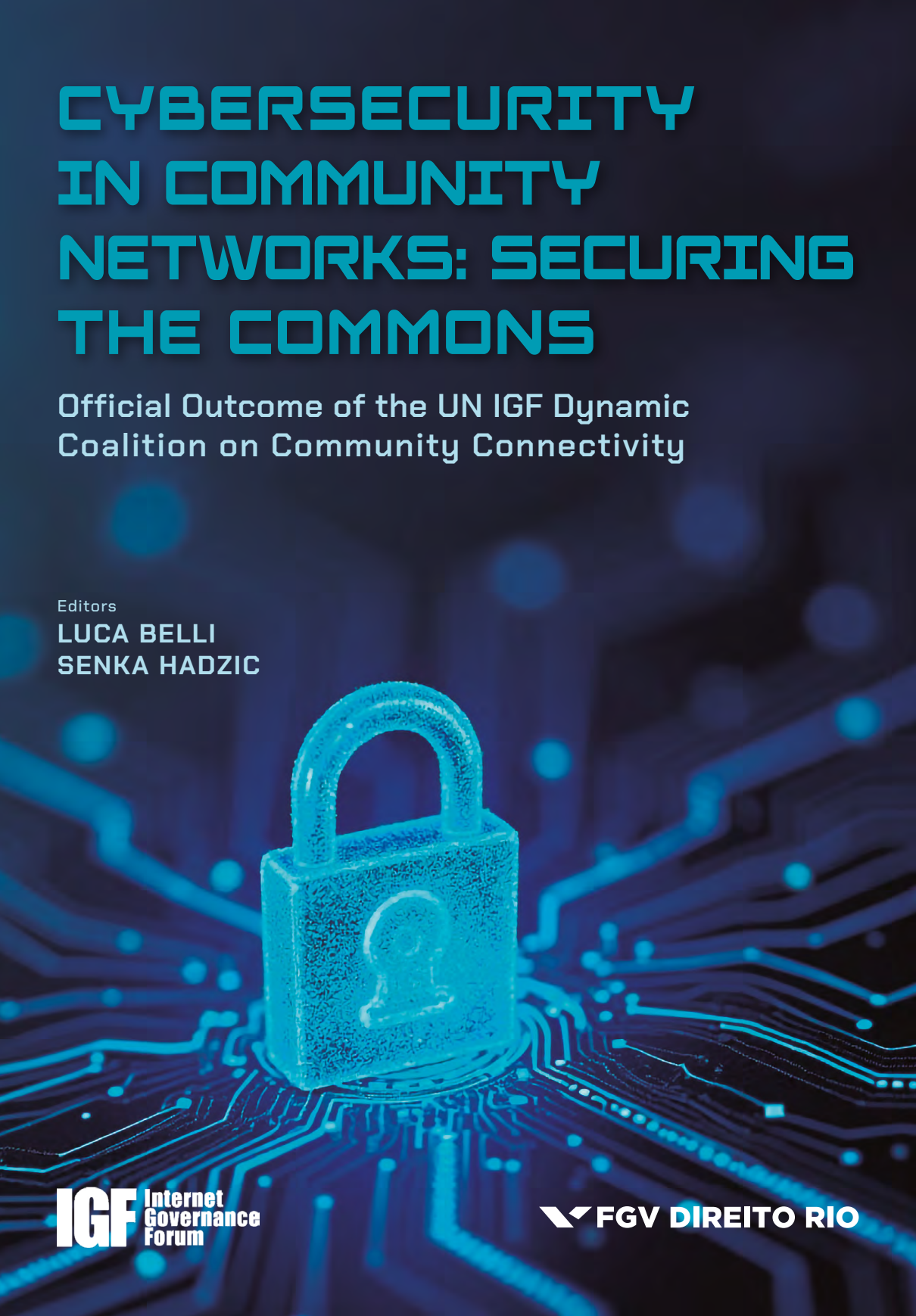
CYBERSECURITY IN COMMUNITY NETWORKS: SECURING THE COMMONS

Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity

Editors
LUCA BELLI
SENKA HADZIC



IGF Internet Governance Forum

FGV DIREITO RIO

Cybersecurity in Community Networks: Securing the Commons

Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity

Edition produced by FGV Direito Rio
Praia de Botafogo, 190 | 13th floor
Rio de Janeiro | RJ | Brasil | Zip code: 22.250-900
55 (21) 3799-5445
www.fgv.br/direitorio

Cybersecurity in Community Networks: Securing the Commons

Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity

Edited by *Luca Belli* and *Senka Hadzic*

FGV Direito Rio Edition

Printed in Brazil.
1 edition finalized in November 2024.
This book is in the Legal Deposit Division of the National Library.

Coordination: FGV Direito Rio
Book cover: Tangente Design
Layout: Tangente Design

Cataloguing data prepared by the Mario Henrique Simonsen/FGV Library

Cybersecurity in community networks : securing the commons : official outcome of the UN IGF dynamic coalition on community connectivity / edited by Luca Belli, Senka Hadzic. - Rio de Janeiro : FGV Direito Rio, 2024.
82 p.

` ISBN 978-65-86060-62-1

1. Redes comunitárias (Redes de computadores) – Medias de segurança. 2. Computadores – Medidas de segurança. 3. Proteção de dados. I. Belli, Luca. II. Hadzic, Senka. III. Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas.

CDD – 341.2732

Elaborated by Márcia Nunes Bacha – CRB-7/4403

CONTENTS

ABOUT THE AUTHORS

Dr Luca Belli is Professor of Digital Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro, where he directs the Center for Technology and Society (CTS-FGV) and the CyberBRICS project. Luca is also editor of the International Data Privacy Law (IDPL) Journal, published by Oxford University Press, and Director of the Computers Privacy and Data Protection conference Latin-America (CPDP LatAm). He is currently member of the Brazilian Presidency's National Cybersecurity Committee, board member of the Global Digital Inclusion Partnership and member of the Steering Committee of the Forum for Information & Democracy. He is author of more than 80 publications on law and technology, exploring data governance, cybersecurity, AI regulation, Internet access, and digital transformation. He has been consulted by several intergovernmental organisations and national regulators, including the Council of Europe, the International Telecommunications Union, the French Telecoms Regulator, etc. and his works have been quoted by numerous media outlets, including The Economist, Financial Times, Forbes, Le Monde, BBC, China Today, The Beijing Review, The Hill, O Globo, Folha de São Paulo, El Pais, etc. Luca holds a PhD in Public Law from Université Paris Panthéon-Assas and can be found on LinkedIn and on Twitter as @1lucabelli

Dr Senka Hadzic is a Senior Fellow at Research ICT Africa, a Cape Town based digital policy think tank. She is also affiliated with the CyberBRICS project at the FGV Law School in Rio de Janeiro where she studies existing regulations, identifying best practices and developing policy recommendations in the area of Internet access (including community networks) and digital transformation in the BRICS countries. Senka holds a PhD in Electronics and Telecommunications Engineering from the University of Aveiro, Portugal and was a postdoctoral researcher at the German Fraunhofer Institute and at the University of Cape Town.

Bruna Zanolli specializes in community-centered connectivity and digital care, drawing on the principles of intersectional feminism, social justice and popular education. She currently leads the Shaping Connectivity area of the Local Networks (LocNet) project, supporting

Communities of Practice, Implementations and Local Services for community networks operating in the Global South, working with the organization Rhizomatica in partnership with the Association for Progressive Communications (APC). She also advocates for the promotion of adequate regulation and affordable funding for community networks in Brazil through Anatel's Community Networks Working Group and the National Community Networks Committee. For over 15 years, she has been working to promote community-led radio and connectivity networks, advocating for technologies and media in the public and community interest, especially focused on traditional and vulnerable territories. Bruna is a former Mozilla Open Web Fellow (2018/19) and a member of the Transfeminist Digital Care Network and APC's Feminist Internet Research Network (FIRN). She holds a master's degree in Communication and Culture from MediaLab UFRJ in Brazil. She is a user and enthusiast of free technologies (FLOSS).

Osama Manzar works at the cusp of Rights, Access and Meaningful Content. He is a Senior Ashoka Fellow, British Chevening Scholar, International Visitors Leadership Program Fellow of the US State Department and an Advisor to Women in Digital Economy Fund (WiDEF). After half a decade of stint in tech journalism, he founded the Digital Empowerment Foundation in 2002, working on "access to rights and rights to access" and digitally empowering more than 35 million people. He was instrumental in several policies and impact activities like India's National Digital Literacy Mission, banning FreeBasics in India, liberalising ISP licensing through PM-WANI in India, and initiating a fight against misinformation with WhatsApp and institutionalising the same. He has been on the boards and advisories of Women in Digital Economy Fund, APC, World Summit Awards, GNI, Barefoot College, Protsahan, MISSING, etc.

Leandro Navarro is senior professor at the Technical University of Catalonia (UPC). At UPC, he is part of the management board of AUCoop, an ICT for development campus association, and co-founder in 2015 of the eReuse.org communitye initiative for the reuse of electronic devices ensuring final recycling involving several refurbishment social enterprises. He was co-chair of the Internet Research Task Force (IRTF) working group GAIA: "Global Access to the Internet for All" (2018-2022). He is an expert in the

United Nations ITU-T SG5 on “Environment, climate change and circular economy” and co-rapporteur of Q7/SG5 on “E-waste, circular economy and sustainable supply chain management”. Since 2023 he is Chair of the Board of Directors of the Association for Progressive Communications. He has participated in numerous ICT events, publications and forums related to the governance of the public internet, community networks, and universal connectivity in Europe and globally.

Suruchi Kumari is a researcher at the Digital Empowerment Foundation. At DEF, her work focuses on research in various aspects of digital rights and citizenships with multiple stakeholders for advocacy and policy-making on the topics of meaningful connectivity and safeguarding digital rights. With an academic background in social exclusion, inclusive policy and geography, her research has focused on urban governance and politics. At DEF, she has been engaged in research design and coordinates the preparation of research and impact reports for various projects related to digital access, education, empowerment, entrepreneurship, etc. Suruchi has MPhil and PhD from Jawaharlal Nehru University.

Ritu Srivastava, Program Officer at IEEE and Director of Jadeite Solutions has over 16 years of experience specifically focusing on the ICT domain, using digital technology towards sustainable development of underprivileged communities /marginalized sections of society. She has extensively worked in areas of digital literacy, digital inclusion, and community networks and supported rural communities to build resilient and scalable bottom-up connectivity models in India. Her research interest lies in areas of rural technologies, broadband policies, gender and access, gender and internet governance, open spectrum policies, digital literacy, and digital health and community development. She has represented India at the United Nations Human Rights Council, and United Nations Secretary General’s High-Level Panel for Digital Cooperation, as well as an organizational representative at the Global Network Initiative. She holds a Master’s degree in Electronics & Telecommunication and an MBA degree in. IT. She is a certified digital security trainer and UN Human Rights Mechanism.

Felix Freitag is an associate Professor at the Technical University of Catalunya (UPC), which he joined in 1999. His research interests include the design of scalable decentralized systems. In the recent years his research focused on in networked distributed and decentralized systems in the IoT, edge and P2P computing, LoRa mesh networks and federated learning.

1 The Need for a Cybersecurity Approach in Community Networks

Luca Belli and Senka Hadzic

Abstract

Community networks (CNs) have emerged as significant connectivity initiatives, especially in underserved regions. These networks, designed and managed by communities, face considerable cybersecurity risks. This paper delves into the multifaceted cybersecurity challenges inherent in CNs, emphasising the existence of large number of cyberthreats stemming from technical vulnerabilities to cyber-attacks, inconsistent security policies, and inadequate risk management practices. It briefly explores the potential data privacy issues, technological limitations, and incident response capabilities, underscoring the need for robust cybersecurity governance. We highlight that legal and regulatory hurdles also present significant challenges, further complicating the cybersecurity landscape for CNs. To enhance resilience against cyber threats, the paper advocates for a proactive, multistakeholder and collaborative approach, highlighting the importance of cybersecurity awareness, training, and investment in security infrastructure. Ultimately, safeguarding the cyber environment and user assets within CNs is crucial for their sustainability and continued growth, ensuring these networks can provide reliable and secure connectivity.

1.1 Introduction

Since 2016 by the Dynamic Coalition on Community Connectivity (DC3) of the United Nations Internet Governance Forum (IGF) has fostered thriving multistakeholder debates dedicated to the analysis of community networks (CNs).[1] DC3 is a multistakeholder group coordinated by Prof Belli and DR Hadzic, aimed at fostering a collaborative analysis of CN initiatives, exploring how they can

1 https://www.intgovforum.org/en/content/dynamic-coalition-on-community-connectivity-dc3-0.

improve and expand connectivity, analysing their technical features, and their governance and funding models.

CNs are crowd-sourced collaborative networks, developed in a bottom-up fashion by groups of individuals – i.e., communities – that design, develop and manage the network infrastructure as a common resource. Hence, CNs are connectivity initiatives managed according to the governance models established by their community members, in a democratic fashion, and may be operated by groups of self-organised individuals or entities such as non-governmental organisations (NGOs), local businesses or public administrations.

This volume aims at tackling a crucial but underexplored viewpoint in the discourse surrounding CNs: the intersection between their functioning and cybersecurity. One of the very rare examples of agreed definitions of cybersecurity is provided by the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) provides a useful and overarching definition of cybersecurity, which is noteworthy for being a rare example of consensual cybersecurity definition at the international level, stating that:

> "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment*[2]*."*

This introductory chapter highlights the relevance of the community network movements not only as an engine for the expansion of

2 See ITU-T (2009).

connectivity but also as a vector of community empowerment, self-determination, sustainability, digital sovereignty, fostering the capacity of previously unconnected community to understand and develop digital technology and enhance their cybersecurity.

The first part of this chapter offers a useful reminder of why CN are interesting options to expand connectivity. The subsequent section provides some insight of the key challenges faced by CN inbuilding cybersecure environments. Lastly the conclusion briefly presents the contributions of this volume.

1.2 Why are community networks relevant?

Over the past years, our research has demonstrated that CNs are a valuable solution to connect people in places that are the hardest to reach by traditional services (so called market failure areas), thus complementing existing connectivity solutions that fail to connect populations living in those areas. Hence, CNs represent a valuable strategy to implement concretely the International Telecommunication Union Recommendation D.19 on Telecommunication for Rural and Remote Areas, according to which "local institutions, such as village committees should be involved in planning and implementing ICT", stressing that "[b]usiness models which can achieve financial and operational sustainability can be operated by local entrepreneurs supported by a variety of initiatives [...] including Universal Service Funds [...]."[3]

Besides offering a significant example of the existence of alternative and valuable approaches to expand connectivity – and, consequently, to fulfil the United Nations Sustainable Development Goals[4] – CNs also offer a demonstration of how Internet governance processes can allow different stakeholders to cooperate, concretely influencing the evolution of the Internet.

Importantly, our research highlights that CNs should not be considered as competing or antagonistic models either to the state or to the

3 https://www.itu.int/rec/D-REC-D.19-201003-I/en.

4 Notably, Goal 9 establishes the United Nations members' commitment to "build resilient infrastructure, promote sustainable industrialization and foster innovation." See https://www.un.org/sustainabledevelopment/infrastructure-industrialization/.

market, but rather as complementary solutions. Our case focuses on CNs, as these initiatives give rise to many positive externalities, enabling sustainable local economies and new governance models, as they expand meaningful connectivity. Our research also highlights that CNs foster the development of low cost open-source software and hardware technologies to connect the unconnected and, consequently, these new Internet users become also producers – rather than mere consumers – of new content and services in local languages, catering to the needs of local communities.[5]

Furthermore, there is widespread recognition that CNs are positive contributors to the local socio-economic environment because, besides providing the capacity to access and share to information and knowledge, they focus on the needs of the local community.[6] In practice this means that, besides being connected to the Internet, local communities start to understand the functioning of digital technologies as they experiment with them, and frequently have a more direct approach with the governance of such technology. Such situation contributes to the development and strengthening of digital sovereignty of the local community through a commons-based approach, where the local communities increase their capacity to understand, develop and regulate their local digital ecosystems, while connecting them to the global Internet.

As emphasised in our research on "Community Networks: Building Digital Sovereignty and Environmental Sustainability", the fact that CNs allow previously unconnected communities to build their own access networks, their community-tailored services, including applications and content in their own local languages, also offering the possibility to organise connectivity through governance models that reflect the self-determination of the local community is a quintessential example of digital sovereignty. In this sense, participants of CNs become digitally sovereign by becoming the

5 See Belli (Ed.) (2016). Community Connectivity: Building the Internet from Scratch Annual Report of the UN IGF Dynamic Coalition on Community Connectivity https://www.intgovforum.org/en/filedepot_download/4391/1163.

6 See the previous reports of the DC3, including a wide number of case studies and analyses illustrating these points, available at https://comconnectivity.org/ as well as in the "Documents and Reports" section of the DC3 official webpage on the IGF website https://www.intgovforum.org/en/content/dynamic-coalition-on-community-connectivity-dc3-0.

"protagonists of their digital futures"[7], as they develop a variety of tools and systems aimed at utilising connectivity to organise the community life in a more efficient and participatory fashion, while reflecting their community values and need into technology. For instance, CN users create billboards for better organisation of the local community, messaging applications in local languages, local e-commerce platforms to trade local products, or e-health applications to share medical information more easily.

Importantly, our research on "Community Networks: Towards Sustainable Funding Models"[8] emphasises that CNs offer a viable alternative to connect populations in settings where traditional models do not fit, i.e., where mainstream telecom operators do not see a business case in investing in remote areas providing service to few households with little purchasing power. CNs are owned and operated by local communities usually relying on low-cost technologies, open-source solutions, and unlicensed spectrum for access provision.

The entire design of CNs differs largely from traditional mainstream networks, as the local communities are involved in the conception, deployment, and maintenance of the CNs. While the specific modalities of CNs establishment and maintenance offer unique advantages in terms of community empowerment, they also present unique challenges in terms of cybersecurity vulnerabilities.

1.3 What are the cybersecurity risks that community networks can face?

As dynamic and inclusive connectivity initiatives managed by communities, CNs have witnessed significant growth in recent years. These networks, developed in a bottom-up fashion, aim to provide internet access in regions where traditional service providers have limited reach.

7 See Belli, L. (2018, March 28). Network self-determination: When building the Internet becomes a right. IETF Journal. https://www.ietfjournal.org/network-self-determination-when-building-the-internet-becomes-a-right/.

8 Belli and Hadzic (Eds). (2021). Community Networks: Towards Sustainable Funding Models. Official Outcome of the IGF Dynamic Coalition on Community Connectivity. https://www.intgovforum.org/en/filedepot_download/92/20438.

Despite their numerous assets, CNs may face substantial cybersecurity challenges that risk undermining their effectiveness and sustainability. This section explores the cybersecurity risks inherent in CNs, emphasizing the need for robust security measures to protect the cyber environment and the assets of organisations and users involved.

1.3.1 Vulnerability to Cyber-attacks

Community networks, given their decentralized and often resource-constrained nature, are particularly susceptible to various forms of cyber-attacks. These include Distributed Denial of Service (DDoS) attacks, malware infections, and unauthorised access to network infrastructure. The lack of centralised oversight and standardised security protocols makes it challenging to implement comprehensive defences against these threats.

In such context, it is possible that bad-faith actors can exploit vulnerabilities in the network's infrastructure, compromising connected devices and accessing sensitive information. The impact of such breaches can be severe, ranging from service disruptions to data theft and financial losses.

1.3.2 Inadequate Security Policies and Practices

The diverse and collaborative nature of CNs can lead to inconsistent security policies and practices across different segments of the network. This inconsistency arises from the varying levels of technical expertise among community members and the likelihood that the CN governance structure is not uniform. As a result, some parts of the network may implement robust security measures, while others may rely on insufficient safeguards. This disparity creates weak points that attackers can exploit, undermining the overall security posture of the network.

1.3.3 Challenges in Risk Management

Effective risk management in CNs can be hampered by several factors, including limited financial resources, lack of specialised cybersecurity knowledge, and the voluntary nature of network administration. Community members may lack the training and expertise necessary to identify, mitigate and react to emerging

threats proactively. Furthermore, the absence of dedicated funding for cybersecurity initiatives can lead to inadequate investment in security infrastructure and tools. Without a comprehensive risk management approach, CNs run the risk to vulnerable to evolving cyber threats that can compromise their functionality.

1.3.4 Data Privacy Concerns

It is important to stress that CNs may handle a significant amount of personal information, making data privacy a critical concern. Once again, the decentralised architecture of these networks may complicate the implementation of uniform data protection measures, when this concern is not backed into the CN culture since the very design of the CN until its deployment and management.

Unauthorised access to personal data, communication intercepts, and information leaks are potential risks that can have severe implications for the privacy of users. In most countries, failure to implement appropriate personal security measures may lead to civil or even criminal liability of the individuals or entities responsible for doing so. Ensuring the confidentiality and integrity of data within CNs requires the full understanding of data protection legislation, security protocols and regular audits to identify and address vulnerabilities.

1.3.5 Lack of Incident Response Capabilities

The capacity to respond effectively to cybersecurity incidents is often limited in community networks. The absence of dedicated incident response teams and predefined protocols can delay the detection and resolution of security breaches. In the event of an attack, the network's ability to contain and mitigate the impact is compromised, leading to prolonged service disruptions and potential loss of user trust. In such a scenario the development of robust incident response capabilities, including monitoring tools and response plans, is essential for enhancing the resilience of CNs against cyber threats.

1.3.6 Legal and Regulatory Challenges

As we discussed in "The community network manual: how to build the Internet yourself"[9], CNs operate within complex legal and regulatory frameworks that vary across regions and countries. Navigating these frameworks can be challenging, particularly concerning cybersecurity regulations and data protection laws, as mentioned above. Compliance with these regulations often requires significant administrative effort and resources, which may be beyond the capacity of CNs driven by volunteers or by poorly resourced organisations. Failure to comply with legal requirements can result in legal liabilities and penalties, further stressing the need for a comprehensive understanding of the regulatory landscape.

1.3.7 Technological Limitations

The technical limitations of CNs, including the use of non-up-to-date hardware and software, can exacerbate cybersecurity risks. Limited access to advanced security technologies and updates can leave the network vulnerable to known exploits and emerging threats.

Additionally, the heterogeneous nature of devices within the network, ranging from legacy systems to modern equipment, complicates the implementation of uniform security measures. Addressing these technological limitations requires ongoing investment in infrastructure upgrades and the adoption of best practices in cybersecurity.

1.4 Conclusion

The cybersecurity risks associated with community networks are multifaceted and demand a proactive and collaborative approach to mitigation. Ensuring the security of these networks requires a combination of technical, administrative, and organizational measures that align with the diverse and decentralized nature of community-driven initiatives.

By fostering a culture of cybersecurity awareness, investing in training and resources, and developing robust risk management

9 Belli, L. (Ed.). (2018). The community network manual: how to build the Internet yourself. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. https://www.intgovforum.org/en/filedepot_download/4391/2376.

strategies, community networks can enhance their resilience against cyber threats. Ultimately, safeguarding the cyber environment and the assets of organizations and users within community networks is essential for their continued growth and success.

This collection of case studies aims at providing an initial understanding of role of cybersecurity governance in community networks, a crucial yet frequently overlooked element in ensuring secure communications for vulnerable communities and securing the "commons" infrastructure. The case studies explore the link between security and community networks in Brazil, India and the European Union.

In the case of Brazil, territories and cultural environments where community networks are located are similarly regarded as common goods, governed and owned collectively. The mapping of community networks in Brazil shows that they are predominantly located in traditional communities, such as quilombolas, Indigenous groups, and riverside populations. These communities face significant vulnerabilities, not only in terms of limited broadband access but also in broader socio-economic challenges. The case study reflects on how community network users are generally more vulnerable to both a lack of meaningful connectivity and greater exposure to information and digital security risks. To promote effective information security and digital care, it's essential to adopt a holistic approach that encompasses the security needs of community networks, including the characteristics of the entire territory, as well as the political and cultural activities within it.

Digital Empowerment Foundation's piece reflects on India's social structure. Being rooted in strong community values, the society often leaves little room for the concept of privacy in non-private community life. Privacy, as an essential aspect of cybersecurity, poses a socio-behavioral challenge. The Digital Empowerment Foundation has been addressing this by raising awareness and providing training to help people understand the importance of privacy in everyday language, aiming to empower individuals to participate in the digital ecosystem as dignified citizens, rather than just consumers of internet infrastructure. Furthermore, with the

growing regulatory landscape around data privacy, data protection, and information handling standards, service providers and organizations are responsible for maintaining ongoing compliance. This shift also highlights the need for a stronger emphasis on cybersecurity at the service level.

Jadeite's CR Bolo empowers community radio stations to leverage connectivity opportunities and offer widespread, meaningful access. This second case study from India highlights a decentralized model of connectivity that helps preserve cultural values while enabling communities to collaboratively shape their internet experience. It underscores the importance of recognizing that such decentralized networks foster a secure and reliable environment, making access to communication services a fundamental right and essential for human development.

The Pangea case study introduces the concept of decentralized digital identity and verifiable credentials tailored for communities, particularly within the social and solidarity economy. Digital service infrastructures such as Pangea.org, Guifi.net community network, or eReuse.org promote the strategic use of the Internet and provide Internet services to the ecosystem to many social and solidarity organizations.

The sections of this study dedicated to design and implementation highlight innovative solutions for building a robust and scalable platform that caters to the specific needs of social and solidarity entities. Risks associated with decentralized digital identity and verifiable credentials are also highlighted, including privacy and security issues, interoperability challenges and concerns about scalability and regulatory compliance stemming from reliance on blockchain infrastructure. The system is built in alignment with regulatory frameworks like eIDAS and EBSI, which establish global standards for decentralized electronic identification and trust services, particularly in Europe but can be applied globally.

The four case studies from different parts of the world show that the intersection of cybersecurity and community networks is a topic that deserves further attention, and needs to be integrated in policy discussions.

1.5 References

Belli et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV (2023). https://hdl.handle.net/10438/33784

Belli (Ed.) (2016). Community Connectivity: Building the Internet from Scratch Annual Report of the UN IGF Dynamic Coalition on Community Connectivity https://www.intgovforum.org/en/ filedepot_download/4391/1163.

Belli and Hadzic (Eds). (2021). Community Networks: Towards Sustainable Funding Models. Official Outcome of the IGF Dynamic Coalition on Community Connectivity. https://www. intgovforum.org/en/filedepot_download/92/20438.

Belli, L. (2018, March 28). Network self-determination: When building the Internet becomes a right. IETF Journal. https://www.ietfjournal.org/network-self-determination-when-building-the- internet-becomes-a-right/.

Belli, L. (Ed.). (2018). The community network manual: how to build the Internet yourself. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. https://www. intgovforum.org/en/filedepot_download/4391/2376.

Dynamic Coalition on Community Connectivity. (2020). *Website of the Dynamic Coalition on Community Connectivity*. https://comconnectivity.org/.

(ITU) International Telecommunications Union (2024). *D.19: Telecommunication for rural and remote areas*. https://www.itu.int/rec/D-REC-D.19-201003-I/en.

United Nations. Sustainable Development Goals. s.d. https://www. un.org/sustainabledevelopment/infrastructure-industrialization/.

2 How to ensure that CNs users have online safety and digital care?

Bruna Zanolli

Abstract

It is common to acknowledge community networks (CN) infrastructure as commons goods, but in Brazil is also true that most of the territories and cultural environment where they are located are also considered common goods and follow collective governance and ownership. Based on a survey of the profile of CNs users and their territories, this text reflects on how these users are also generally more susceptible to a lack of meaningful connectivity and more exposed to vulnerabilities related to information security and digital security. Thus, in order to promote information security and digital care, it is important to have a holistic perspective on the security needs of CNs, adding their entire territory caracteristics, and political and cultural activities as axes that need to be secured as a whole, considering their profiles, lifestyles and potential risk, meeting their specific needs, by understanding that a CN is only as secure as its users can be.

2.1 Introduction

Initially, the text presents the profile of those who connect to the Internet through community networks in Brazil and the particularities of their territories, reflecting on how these users are also generally more susceptible to a lack of meaningful connectivity and more exposed to vulnerabilities related to information security and digital security.

Then, looking at their territory configuration, we explored the fact that in Brazil most CNs are considered common goods because of the land they occupy and their traditional origins, following collective governance and ownership. Therefore, that also reinforces their CNs nature as commons. Based on both those facts, we explore the vulnerabilities to which they are subject and their particular strenghts to mitigate it.

Closing with recomendations to have an holistic perspective on the security needs of community networks. Considering that to promote information security and digital care, their entire territory and cultural activities should be taken into account, combined with understanding their profiles, lifestyles and potential risk and meeting their specific needs.

2.2 Community Networks users profile

According to the Community Internet Networks in Brazil survey[10] (CGI.br, 2022), 70% of Brazilian community networks are located in municipalities with a Gross Domestic Product (GDP) per capita below the national level (of these, a third are among the 25% of the country's poorest municipalities). And almost half of the networks are located in the municipalities with the worst school performance among children and young people in the public school system, both for basic, primary and secondary education. Thus, the socio-economic profile of users of community networks is that they are found in areas of greater social vulnerability, with a significant presence of poor families and poor economic and school performance (CGI.br, 2022).

Considering the territories where the networks operate, 82.5% of the networks are in territories with traditional communities, of which 40% are in quilombos or quilombola territories, 32.5% in indigenous villages or territories and 22.5% in riverside areas and 32.5% in other areas with traditional populations such as settlements, extractivist communities, caiçara communities, among others. Community networks in Brazil are therefore found in traditionally excluded and historically vulnerable regions and localities. The majority of their managers are self-declared black and brown (55%) and 20% indigenous (CGI.br, 2022).

Also, in relation to broadband access, the networks are located in areas with low access density, where 66% are in municipalities with only up to 10 accesses per 100 inhabitants and 15% in municipalities with between 11 and 20 accesses. And although we don't have data

10 REDES COMUNITÁRIAS DE INTERNET NO BRASIL: experiências de implantação e desafios para a inclusão digital, Comitê Gestor da Internet no Brasil, CGI.br (2022). Available at: https://www.cgi.br/media/docs/publicacoes/7/20220905125048/estudos_setoriais_redes_comunitarias_de_internet_no_brasil.pdf.

comparing the availability of mobile data signals and the number of Base Transceiver Station (BTS) in the municipalities where the networks are located, it is usual that the only realiable and/or affordable connectivity is the one provided by a community networks, especially in regions that are geographically more distant or isolated from large urban centers.

In other words, in areas where connectivity is available through community networks indicates that their users are part of a population group with greater socio-economic vulnerability, lower educational attainment and historically marginalized populations. And just as the people most affected by the lack of connectivity are the most vulnerable, these same profiles are the main targets in terms of lack of online security.

To reinforce this point, the national indicators of meaningful connectivity (CGI.br, 2024)[11], which consider pillars such as infrastructure, affordability, device, skills, protection and security, state that 78% of Brazilian Internet users do not have meaningful connectivity. And the data confirms a socio-economic profile of people with less significant connectivity very similar to those found in community networks, where poor people, black and brown people and residents of rural regions have the most precarious access. Part of the framework considered to qualify meaningful connectivity includes technical skills such as installing applications or programs and attaching files to messages, and skills for safe and reliable use of the Internet, including measures for security of use, safeguarding privacy and verifying the information accessed (CGI.br, 2024). This confirms that, in general, less schooling means less access to information and/or information integrity and less ability to process information, fewer digital skills and less privacy; and also, economic precariousness means shared and/or older devices, with fewer resources and potentially more vulnerable to attacks.

Thus, although users of community networks may have access to basic connectivity, they do not fit into the national profile of users who access meaningful connectivity, i.e. with a fast and reliable

11 *Meaningful connectivity: measurement proposals and the portrait of the population in Brazil,* CGI.br (2024). Available at: https://bibliotecadigital.acervo.nic.br/items/6a57c554-c067-4f8b-a6f4-f53717ec637b.

signal, their own suitable device, secure browsing and adequate skills (CGI.br, 2024). What makes these profiles more susceptible to phishing for personal information and passwords, poor privacy settings on social media accounts and messaging apps, insecure browsing and email, virus, ransomware and malware, as well as greater exposure to malicious content, financial scams, gambling sites and promises of easy money that lead to debt, and the spread of misinformation, among others.

And, just like offline, there is an intersection of vulnerabilities when we add other forms of power imbalances to all the problems already faced by women, racialized bodies, people with disabilities, LGBTQIAPN+ communities and immigrants in online environments. So, once again as a reflection of the profiles most targeted by other forms of violence and insecurity offline, people in community networks are also susceptible to sexism, ableism, xenophobia, misogyny, racism, and the various forms of prejudice and violence we fight against every day, reinforced by the internet and intertwined with the profile described above.

2.3 Combined commons

As we have seen, the mapping of community networks in Brazil indicates that they are mostly found in traditional communities - such as quilombolas, indigenous and riverside communities. The 1988 Brazilian Constitution recognizes the rights of traditional peoples and guarantees the demarcation of the territories they occupy. In both indigenous and quilombolas cases, the process is collective, starting with a group of residents who benefit from the individual and collective usufruct of the land and are responsible for its collective management, which may continue to be owned by the Union (in the case of indigenous lands) or adopt a collective ownership regime for associations of residents (in the case of quilombola lands). In this way, these territories can be considered common goods, both because of the nature of their ownership and/or usufruct, as well as because of the collective governance of their resources, mostly exploited by family farming and livestock, artisanal fishing and agro-ecological extraction.

This notion of commons is also seen in community networks, from their conception to their maintenance, with the involvement of both the community and partner organizations, with financial donations, equipment and technical support. The participation of community members in decisions is notable in most networks, which reinforces it as a fundamental element for the sustainability of these experiences (CGI, 2022). In addition, the non-profit nature and collective management of the networks reinforces their nature as commons.

We can thus see that in Brazilian community networks, most of which are located in traditional territories and/or managed by traditional population, there is an overlap between both these commons notions, where the collective governance of territories serves as the basis for the collective governance of community networks. In this context, while community networks are common goods managed collectively by the community and its leaders, they also serve the purpose of ensuring that the other common goods of these territories - such as the preservation of the land, local culture, ways of life and traditional knowledge – benefits from online communications and advocacy, in an active and communal way.

This is because most active CNs have Internet access and the communities, in the perception of their managers, use them for various functions, such as promoting their cultural activities, spreading campaigns, mobilizing members, reading the news, studying and working (CGI, 2022). As such, there is the potential for community networks, while ensuring the governance of the commons of their connectivity infrastructures, to use the internet and local value-added services, to also reinforce the other commons of these territories.

2.4 Socio-environmental protection and community networks

It is well known that in regions where connectivity is lacking, the vast majority also lack other essential rights, such as the right to housing; to work and income; to sanitation, drinking water and electricity; to land; to gender and racial equality and to leisure and culture. Against this backdrop, CNs are an alternative form of connectivity that can support access to communication and the internet and the exercise of social, economic and political rights. Weaving networks

that are not only digital, but also social[12] (APC, 2021). That's why it's not uncommon for territories that promote community networks to also do so to support local activists and defenders of human rights, climate justice and the right to land, and the struggles of black, indigenous and women's movements.

The same internet that serves as a tool for basic communication, access to education, health, work and income, socio-environmental protection and can even play a central role in enabling processes to denounce human and environmental rights violations. However, it can be an instrument for exposing and making communities and their defenders vulnerable, spreading disinformation, encouraging cultural alienation through harmful content, manipulating public debate and democracy, and even recruiting and protecting perpetrators of environmental crimes, such as illegal mining and deforestation.

An example of this is the use of Starlink by gold miners and illegal logging in the Amazon region, where seizures of their antennas being a constant occurrence in government operations to repress environmental crimes, in Yanomami Indigenous Land alone, 50 Starlink antennas were seized from March to July 2024[13]. Due to the ease of transportation and the lack of control over who is actually responsible for the equipment, 90% of seized Starlink antennas are registrated by straw man, an easy and unexpensive process the government has been trying to address unsucesfuly with Starlink[14]. Another aspect to be taken into account for internet users and defenders who live in regions with community networks and/or with connectivity restricted to only low-orbit satellites or a single local provider, resulting in a lack of communication alternatives in the event of a connection failure or intentional depredation of the infrastructure. In addition to Internet packages more limited than fixed broadband and security vulnerabilities present in their low-orbit satellite connection, for example[15].

12 MANUAL DE REDES COMUNITÁRIAS. APC 2021. Available at: https://www.apc.org/sites/default/files/manualredescomunitarias.pdf.

13 https://apublica.org/nota/ibama-apreendeu-antenas-starlink-em-3-terras-indigenas-e-garimpos-ilegais-em-4-estados/.

14 https://apublica.org/2024/07/elon-musk-starlink-resiste-a-mudar-identificacao-de-compradores-de-antenas-na-amazonia/.

15 https://www.wired.com/story/starlink-internet-dish-hack/.

At the same time, the same infrastructure is often used, but in a legalized way, by members of CNs in the Brazilian Amazon region and in indigenous and quilombola territories, to denounce violations of their land, territorial and human rights, risking their lives and many have already received death threats from local militias several times. In this context, knowledge about cyber security can literally save lives and play a key role in strengthening social and environmental movements and expanding their capacities and reach.

Common ways of reporting these socio-environmental violations are to take photos and videos of crimes in the act with a cell phone, to record audios of clandestine meetings that gather people to commit crimes, and to communicate with journalists and socio-environmental protection organizations through online messengers. All of this, if done without taking the necessary digital precautions and identity protection, can serve as a death certificate for the defenders when they fall into the hands of local militias. And it's not even necessary for them to physically access devices in order to identify the defenders. Often, the use of social networks and messaging apps without due care and identity protection, making it easier to locate them and leaving their profiles publicly exposed, can already serve as a trigger for identifying and locating the defenders. This is in addition to the aforementioned challenges of old cell phones, which are often outdated and vulnerable, lacking the memory to install new apps, and also lacking the literacy and training to use anonymity apps, secure media and reporting apps, which are often only available in foreign languages and are difficult for users to experience.

Thus, the difficulties faced by human rights and environmental defenders are multiple and complementary. In addition to those mentioned on a personal level, they are reinforced by the lack of efficient public support and structure for reporting and rapid response for threatened people, coupled with the presence of violent local militias that have abundant economic and informational resources. This reinforces the fact that threats that happen online can escalate to physical ones, understanding that it is no longer possible to treat the online environment as being disassociated from its offline

consequences. Because what happens on the internet is a reflection of the world outside it[16].

Precisely because they are people who are already targeted and/or deal with sensitive topics, it is essential that they have at least basic knowledge of how the Internet works and what potential risks and exposure they are subject to online. Specially on the use of secure communication apps, awareness to use social media and commercial platforms in a way that their exposure and personal identities are mitigated and to manage safe data storage and sharing.

2.5 Conclusion

As we have seen, the mapping of community networks in Brazil indicates that they are mostly found in traditional communities - such as quilombolas, indigenous and riverside communities - with high levels of vulnerability, both in terms of access to broadband and in socio-economic, with a lack of access to meaningful connectivity. Having in mind that online safety and digital care is a difficult subject for most people, not just those in community net online safety and digital care?" is essential.

Throughout this text we have come to understand the profile of people who use CNs and defenders of their territories, so it is very necessary for training resources to have in mind methodologies that can really get close to people, understanding their culture and ways of learning, such as the popular education framework[17]. This is because it is not uncommon to hear reports of defenders and CN users who have been through digital security courses but have ended up feeling more confused, insecure and less able to deal with digital exposures and securing their daily tasks. A holistic

16 An action-research made by a group of people, including the author, that supported the implementation of a women-led CN in the quilombola territory of Ribeirão Grande/Terra Seca, part of the Feminist Internet Research Network, has reflected upon digital security and created a digital care zine to distribute to the community. Available at: https://firn.genderit.org/sites/default/files/2022-03/zine01.pdf.

17 Popular Education is an educational framework in Latin America that values people's prior knowledge and their cultural realities in the construction of new knowledge. Educator Paulo Freire was a great supporter of this approach, which encourages the development of a critical look at education and the participation of the community as a whole, encouraging dialogue and guided by the perspective of realising all the rights of the people. The teaching-learning process is seen as an act of knowledge and social transformation, recognising the importance of popular and scientific/technological knowledge.

approach to digital security, which involves information security, digital care and continuous training that is culturally relevant - is urgent in this context.

In addition, it has been documented that the factors that guarantee the sustainability of the CNs are: the participation of local actors in decisions about the functioning of the networks; the training and education of people from the community to maintain the activities; the promotion of self-management; and the support of external organizations that promote the agenda to maintain the activities and access resources and information that are not available in the localities (CGI, 2022). It is therefore necessary to include digital care as another axis to guarantee not only CNs sustainability, but also their users online and offline security.

Also fundamental, is to understand that connectivity and the Internet are not an end in themselves and in most communities they are used as tools in socio-environmental struggles and to promote other human and environmental rights. Therefore, there is no point in guaranteeing that only the physical and logical infrastructure of community networks is secure, it is necessary that their users have the ability to make meaningful and secure use of the network, so that it does not become yet another element of vulnerability, adding more fragility to communities that are already historically marginalized.

This does not diminish the need to also make efforts to ensure that all infrastructure, and especially local and sensitive data, is secure in its storage and sharing, especially considering the benefits that local value-added services can bring to communities, such as local mapping through geolocation and the use of sensors to generate socio-environmental data and strengthen local production, access to local platforms with relevant content on the solidarity and circular economy, health and education, the production and dissemination of local and culturally relevant content, among others. Which must not only follow best practices in relation to data management, but also comply with national data protection laws, since non-compliance can be a week point in case of a targeted persecution of a CN.

In addition, the combined commons nature pointed before of most CNs, could potentially greatly benefit training in digital care and

the adjustments needed to ensure online and offline security. This is because the logic and practices of collectivity, when well worked out, facilitate the local dissemination of information and collective organization mobilizes the community socially and politically to address the needs raised.

Thus, based on the reality of each territory and community network, considering all its complexities and historical legacy, it is a matter of working to mitigate the risks of connectivity based on the uses relevant to each CN, using the notion of informed consent, where the choices made about the digital technologies and resources to be used involve their benefits as well as their risks. To ensure that digital security and meaningful access can also include the right to self-determination of networks, considering greater autonomy and co-participation not only in the connectivity infrastructure but also in its uses, enhancing its benefits and mitigating its harmful consequences.

2.6 References

Burgess, M. (2022). *The hacking of Starlink terminals has begun*. https://www.wired.com/story/starlink-internet-dish-hack/.

Cavalcanti, G. (2024). *Mapa das apreensões: locais onde o Ibama confiscou antenas Starlink*. [online] Agência Pública. https://apublica.org/nota/ibama-apreendeu-antenas-starlink-em-3-terras-indigenas-e-.

MANUAL DE REDES COMUNITÁRIAS. APC. (2021). https://www.apc.org/sites/default/files/manualredescomunitarias.pdf.

Meaningful connectivity: measurement proposals and the portrait of the population in Brazil, CGI. br (2024). https://bibliotecadigital.acervo.nic.br/items/6a57c554-c067-4f8b-a6f4- f53717ec637b.

REDES COMUNITÁRIAS DE INTERNET NO BRASIL: experiências de implantação e desafios para a inclusão digital, Comitê Gestor da Internet no Brasil, CGI.br (2022). https://www.cgi.br/media/docs/publicacoes/7/20220905125048/estudos_setoriais_redes_comunitarias_de_internet_no_brasil.pdf.

Valente, R. (2024). *Starlink: 90% de antenas em garimpos estão em nome de laranjas*. Agência Pública. https://apublica.org/2024/07/elon-musk-starlink-resiste-a-mudar-identificacao-de-compradores-de-antenas-na-amazonia/#:~:text=O%20procurador%20da%20República%20em,registradas%-20em%20nome%20de%20laranjas.

3 Decentralized digital identity and verifiable credentials for communities

Leandoro Navarro and Felix Freitag

Abstract

This paper presents the concept of decentralized digital identity and verifiable credentials for communities, the design of a software system to support the needs of communities in the Social and Solidarity Economy, emphasizing the importance of secure and efficient identity management. The system is developed within the context of decentralized digital identity and verifiable credentials considering the regulatory frameworks of eIDAS and EBSI, which set the standards for decentralised electronic identification and trust services in Europe but applies globally.

The system is designed to integrate seamlessly with existing infrastructures, ensuring compliance and interoperability. Sections on design and implementation highlight the innovative approaches taken to build a robust and scalable platform capable of handling the unique requirements of social and solidarity entities and communities.

Evaluation, including testing and real-world pilot deployments, validate the system's effectiveness and usability. The discussion section delves into the preparation of case studies and pilots, showcasing the practical applications and benefits derived from the system. It also addresses the challenges encountered and the lessons learned throughout the development and deployment phases.

By comparing our work with related research, we underscore the novelty and significance of our contributions to decentralised identity and credential management for communities in the social and solidarity sector. Our findings offer insights for practitioners and policymakers who leverage technology to enhance security and efficiency in digital identity and credential verification processes working with vulnerable citizens and communities.

3.1 Introduction

This paper provides an analysis of opportunities and requirements for decentralized digital identity and verifiable credentials for communities, the challenges faced and the solutions devised during the development, testing, and implementation phases of IdHub[18], a software project to provide identity and credential management systems for organizations supporting activists and marginalized citizens, including community networks, computer reuse communities and other Social and Solidarity Economy (SSE) initiatives. The project encountered significant hurdles, notably the integration of various software modules and libraries, necessitating custom workarounds and extensive testing regimes. Automated testing suites were integrated into a Continuous Integration pipeline to ensure robustness and performance.

Firstly, the W3C Decentralized Identifiers (DID) and Verifiable Credentials (VC) technologies represent a groundbreaking shift in how digital identity and trust are managed on the internet.

According to (W3C, 2022) a DID is a globally unique identifier that enables an entity to be identified in a manner that is verifiable and does not require a centralized registry. DIDs enable a new model of decentralized digital identity that is often referred to as self-sovereign identity or decentralized identity. A DID looks like a unique, decentralized identifier (e.g., did:web:guifi.net:alice) with an associated private and public key, equivalent to a unique email address with PGP keys or a personal web page where a public key can be found.

A VC is a signed digital credential containing claims about a subject, such as identity or qualifications, verifiable through a cryptographic signature. An example of a credential issued by a guifi.net authority with a claim Alice is a member that day:

18 Website: https://IdHub.pangea.org.code repository: https://farga.pangea.org/ereuse/IdHub. A joint project by Pangea.org and UPC.EDU with the support of the NGITrustchain project.

```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "type": ["VerifiableCredential"],
  "issuer": "did:web:guifi.net",
  "issuanceDate": "2024-09-05T00:00:00Z",
  "credentialSubject": {
    "id": "did:web:guifi.net:alice",
    "type": "CommunityMember",
    "membership": {
      "network": "guifi.net",
      "role": "Member"
    }
  },
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2024-09-05T00:00:00Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:web:guifi.net#keys-1",
    "jws": "eyJhbGc..example.signature"
  }
}
```


Individuals, organizations, and devices can create unique, self-sovereign identities as DIDs that are not dependent on any central authority. Paired with VCs, these technologies allow an issuer DID to issue cryptographically secure credentials, easily verifiable by any third party, without compromising privacy under some conditions. The decentralization inherent in DIDs eliminates the need for intermediaries, enhancing user control and resilience. Moreover, W3C standardization ensures global interoperability, fostering trust across systems while empowering users to share only the data necessary for verification. This combination of privacy, verifiability, and decentralized control marks a significant evolution in digital identity management.

We aimed to provide a starting point for communities for an easy-to-use, open-source, standards-compliant implementation of a decentralized digital identity and verifiable credentials web services. This was developed as idHub (idhub, 2023).

A critical aspect of the project was developing admin-friendly data import mechanisms for IdHub to facilitate **credential issuer organizations** to generate identities and credentials about multiple persons (volume data entry). For instance, before a training activity or when participants join a community, the administrator of an organization can create a new decentralized identity for all or

several participants. After the training, an issuer organization creates a verifiable credential for each participant. This involves automating the generation of spreadsheet template files based on VC schemas (credential templates) and data validation processes. By filling specific participant data in a template spreadsheet file associated with one credential schema and uploading it to IdHub, the system issues a credential for each individual in spreadsheet rows, including all credential fields in the columns. As a result of this process, each participant receives an invitation by email to access their decentralized identity wallet and will find all credentials issued to them.

Participant **individuals** access their **identity wallet** hosted in a given identity service provided by an issuer organization. It looks like a webmail service, where after login, an individual can access its identity wallet containing the credentials they have received from other credential issuer organizations[19]. That individual can decide to present that credential to any verifier organization to accredit that information. This is done using the OpenID for verifiable presentation standard protocol.

Third-party organizations can offer web services, a **credential verifier organization portal**, where visitors can securely present their credentials to accredit their identity or any other credentials they received from any issuer organization. This way, a verifier web service can immediately confirm specific details come from the right person, the credential was issued by a given issuer organization, and is still valid (not revoked). In some cases, the issuer organization was accredited to issue these credentials.

Decentralization in DIDs offers more autonomy and global interoperability compared to traditional digital signature systems, like those regulated by eIDAS in Europe, by enabling individuals and organizations to create and verify identities without relying exclusively on national public authorities, fostering broader trust and resilience across borders. This is especially beneficial for vulnerable populations, such as migrants or gender-diverse individuals, who

19 Consider DID equivalent to email/web addresses (alice@guifi.net can be did:web:guifi.net:alice) and credentials equivalent to signed emails in their identity inbox.

may face challenges with national identification systems, allowing them to establish secure and portable identities on their own terms.

The project tackled the complexities of setting up diverse pilot scenarios, employing DevOps practices and CI/CD methodologies to manage multiple software versions and configurations efficiently. Engaging with communities of practice for pilots posed further challenges, requiring alignment with stakeholders' needs effectively.

Feedback from pilot organizations testing an IdHub deployment highlighted the flexibility and ease of use of the developed tools, enabling process scalability and efficiency gains. However, the project also recognized the potential barriers introduced by digitalization and the concept of decentralized identifiers, especially for vulnerable sectors.

Overall, the project's outcomes aligned with its initial goals, offering a tailored identity management solution that supports organizations in empowering marginalized groups. This paper provides detailed insights into the project's technical achievements, business model, exploitation strategies, and future directions, underscoring its contribution to enhancing identity verification processes and fostering inclusivity.

The rest of this paper is structured as follows: Section 2 introduces the needs of the social and solidarity economy and then explore the context of eIDAS and EBSI in Section 3. We discuss the system architecture in Section 5, leading into the system's design and implementation. The evaluation in Section 6 covers testing and pilot validations. The discussion in Section 7 includes case preparation, benefits, challenges, and lessons learned. Related work in Section 8 situates our research within the current work, leading to conclusions in Section 9.

3.2 Needs of the social and solidarity economy

The ecosystem we address is usually called the social and solidarity sector (SSE) (Borzaga, 2019). In this sector, organisations promote equitable, sustainable and rights-based socio-economic development in their community, taking special care of marginalised people. Marginalised populations can vary depending on the context and

region. However, common categories often referred to as marginalised are minorities, people living in poverty, homeless individuals, immigrants and refugees, the LGBTQ+ community, persons with disabilities, the elderly population, and indigenous peoples.

The work of social and solidarity organisations is crucial in alleviating poverty and contributing to social integration and cohesion. These organisations also empower and give voice to marginalised groups, promoting their inclusion and providing access to information, communication networks, and resources. That is the area where internet activists come to help. This is the case with digital service infrastructures such as Pangea.org, Guifi.net or eReuse.org, which promote the strategic use of the Internet and provide Internet services to this ecosystem to many social and solidarity organisations.

The core business domain focuses on designing and implementing an identity and credential management system tailored to organisations working with activists and marginalised citizens. This system draws inspiration from Pangea's and Guifi.net's digital services and circular device management services.

The challenge we aim to address is the centralisation of digital identity-related information and the absence of automated data accreditation mechanisms across organisations within our community. Currently, our members rely on simple identification methods, such as usernames and passwords. However, these methods are no longer sufficient due to the growing need for more decentralised, verifiable, secure, privacy-respecting, and user-friendly ways to manage identity-related information for authentication, authorisation, and accreditation. By leveraging Verifiable Credentials and OpenID Connect technologies combined with shared credential schemas and related services, such as the one proposed by the EU public European blockchain services infrastructure (EBSI), we can foster a trust chain that brings significant benefits. This approach empowers organisations and their members within our business domain to engage in federated interactions. These interactions allow access to different organisations' services or benefits, extending even to third parties beyond our community. For instance, a member of one

organisation should be able to access a service offered by another organisation without disclosing extensive personal information or full credentials. They should also be able to present a verifiable accreditation issued by their organisation to immediately access benefits such as social support, discounts, job opportunities, or other offerings from various public or private organisations. This approach enhances user privacy and convenience, addressing the main challenges in our business domain.

We build on the experience of several NGOs and community networks in different global north and global south countries that provide internet and ICT services to other NGOs, individuals and organisations that work on change, social justice, education, peace, the environment, development, cooperation, etc. Several of these organizations were involved in the co-design of the system (Sabiescu, 2013).

The experience from the previous specific scenario leads to propose a generalised scenario where:

- Affiliated people relate to and interact with multiple organisations.
- Organisations can build trust relationships with each other, including public and private organisations such as NGOs, community networks or social enterprises. This trust can facilitate the exchange and verification of the data and claims each can issue about people.
- Organisations offer services to people and each other.
- Organisations would like to have control over their claims (credentials).
- Individuals want control over their identity, personal information, and credentials they collect from and present to organisations and services.
- Individuals would like to simplify interactions and increase trust in the information they share with organisations by supplying verifiable claims about membership, training and other accreditations.

In this generalised scenario, a person linked to an organisation could interact with another organisation and be able to prove to the latter something granted by the former without revealing unnecessary data or the risk of giving away their identity credentials without consent.

3.3 Context: eIDAS and EBSI in Europe and globally

The European Blockchain Services Infrastructure (EBSI), a public sector blockchain service enabling secure and efficient cross-border transactions between the public and private sectors, is crucial in transitioning from eIDAS1-qualified signatures (EIDAS, 2014) towards eIDAS2 (EIDAS, 2024), based on verifiable credentials. This would align with the goal of eIDAS2 to move away from nationally issued digital identities towards electronic attestations of valid attributes at the European level. This focus on verifiable credentials provides a way to verify these claims in a decentralized manner.

This change necessitates the provision of digital wallets capable of linking national digital identities with proof of other personal attributes and other tools and services for issuer and verifier roles (EP, 2022), as well as the technological transition issues that add to it. Our work contributes with working solutions adapted to the needs of our specific sector.

Lastly, the technical implementation work started alongside the legislative process. The toolbox procedure established to guide this process involves cooperation between Member States, the Commission, and other stakeholders. However, this procedure will produce several implementing acts defining a technical architecture and reference framework, common standards and technical specifications, and common guidelines and best practices. These results will be adapted as necessary to the outcome of the legislative process (EP, 2022), but this is a source of delay and uncertainty in the eIDAS2 scenario. Anyway, while targeted to European needs, it adheres to W3C standards, ensuring its applicability and interoperability on a global scale.

This has led us to design credential schemas and a trust and accreditation model aligned with EBSI credentials, attestations, and trust models. This can enable the SSE to participate in the European public infrastructure and interoperate with EBSI, as well as work globally.

3.4 Identity and credential management system

The identity management system we propose to build aims to satisfy these specific and generalised needs the following:

1. Organisations can associate information (attributes, roles, and other details) to persons (subjects) they are involved with for a purpose (e.g., registering a user to access and provide them internet services, registering an employee, member or beneficiary of an organisation to entitle her to benefits provided by the same or another organisation).
2. Organisations can issue credentials to subjects according to the information they manage.
3. Subjects can exercise their rights regarding the information held by organisations.
4. Subjects can present credentials to interact with a party.
5. Third parties should be able to verify claims contained in verifiable presentations to award subjects a benefit (service). (e.g., access community-centred internet services, social benefits, discounts, register as a member)
6. All actors should agree on a common information model regarding credential types and credential schema, including structure, format, validation and revocability.

We have explored and looked at integrating existing and emerging technologies (DID Key and Web schemes, single sign-on, federation, OpenID, verifiable credentials) to facilitate, automate and provide verifiability for each organisation's management of identity-related information about its people. This way, organisations can issue credentials about subjects, and subjects can manage and present their credentials to other parties for information and verification. We aim to create a more understandable, easy, efficient, and scalable way to manage decentralised identity, promoting autonomy, trust, privacy, and verification to credential data, adapted to the needs of the social and solidarity economy for the socio-economic inclusion of citizens, particularly the most vulnerable.

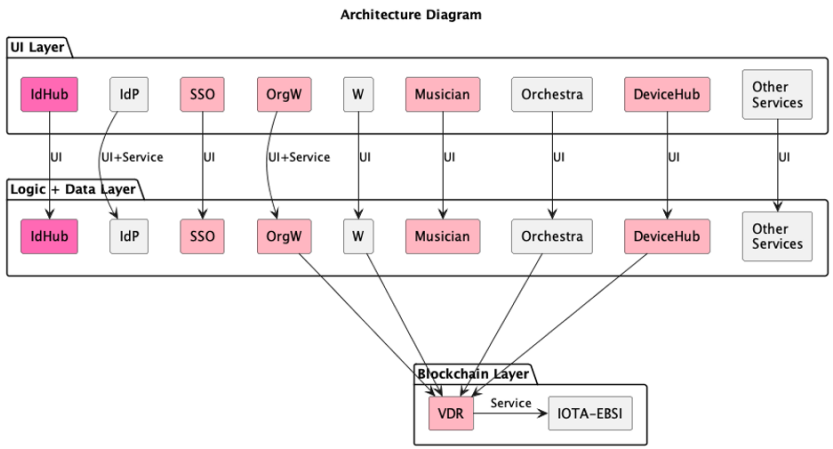
This system should ease users' understanding of which details they provide about them in their interactions in the digital world with other parties. For instance, individuals can decide to present the

credential that matches the minimal details required by a verifier organization[20]. This understanding by users and the credibility of the provided information should simplify interactions with service providers. That can improve the lives of communities of citizens using digital devices and services. This is aligned with emerging decentralised identity models, considering eIDAS2 and building on existing standard technology solutions, but not adapted to the SSE and similar communities of practice.

3.5 System architecture

A simple architecture diagram is in Figure 1. Pink blocks represent new developments (foreground) as new blocks or extensions of background blocks (light Pink), and grey blocks those unmodified but used perhaps with modifications for integration. The IdHub module integrates most development tasks, as it is a hub for managing people's information to feed the issuance of verifiable credentials.

Figure 2 Software architecture of IdHub



20 An issuer can provide a holder with a set of credentials with different levels of detail so holders can choose the right one to present to a third party to minimize personal data transfer. Selective disclosure credential presentation mechanisms allow for that, but these are not yet implemented in our code.

The technical components or modules are detailed in Table 2.

Table 1 Technical modules in IdHub

Acronym	Description	Parts	Work to do
IdHub	Organisational identity management system	UI, logic, data	develop
IdP	Identity provider service: per organisation	UI+service, logic, data	develop + existing libs
SSO	SSO portal (part of the IdP)	UI+service, logic, data	develop/ integrate
OrgW	Credential org wallet: issue, verify credentials	UI+service, logic, data	develop + existing libs/ integrate
Shop	Devices' online shop portal	UI, logic, data	extend
Musician	Service control panel	UI, logic, data	extend, integrate
Orchestra	Resource and service management service	UI+service, logic, data	extend, integrate
DeviceHub	Device management service	UI+service, logic, data	extend, integrate
VDR	Verifiable data registry	Service, smart contracts, ledger	extend, integrate
Services	Integration of credential authentication in third-party services/applications	?	extend, integrate
W	Credential holder identity wallet: hold, receive, present credentials	UI, logic, data	Integrate (use)
EBSI	EBSI services: identity, trust, registry	Service, ledger	Integrate (use)

The architecture is broken down into three logical layers and components and defines their interactions. These are:

- Presentation layer (UI): Includes user and/or service interfaces for the various components, such as web interfaces for the service control panel, online shop portal, organisational identity management, identity provider, and credential wallets.
- Business logic layer: Contains the core logic and functionalities of each component, including the SSO portal, identity provider related to authentication and validations of credentials, resource and service management (Musician, Orchestra, DeviceHub),

and several organisational identity management and credential management (IdHub, OrgWallet, Wallets and EBSI).

- Data layer: Manages the storage and retrieval of data the components require. It can rely on a database or data store (files, encryption) or a ledger for a verifiable registry (VDR).
- Regarding the interactions and communication between components:
- The SSO portal handles user authentication and provides single sign-on capabilities to all user-facing services.
- The service control panel (Musician) and online shop portal interact with the SSO portal for user authentication and authorisation.
- The resource and service management service (DeviceHub, Orchestra) communicates with the service control panel (Musician) and online shop portal to manage resources and services.
- The organisational identity management web UI (IdHub) uses the data layer to display member information.
- The credential management component (OrgW) issues and verifies credentials. It interacts with any service that requires identification or accreditation (e.g., SSO/IdP, verifiable registry (VDR), and integration layer to other services).
- The credential holder wallet (W) receives and presents credentials and communicates with the SSO portal and credential management component.
- The verifiable registry stores and provides a ledger of main transactions done.
- Additional integration logic is required to integrate authentication and credential verification with third-party services and applications.

The software was developed using an agile methodology. This allowed the team to deliver valuable working software frequently and adapt to potential changes. The application was tested using a combination of unit, integration, and system tests, which ensured its reliability and meeting of user requirements.

3.5.1 Implementation

IdHub is a Django-based application structured around 8 key components in Figure 2. Each component represents a separate module or application within the larger project, following Django' "reusable applications" principle.

Table 2 IdHub elements as directories in the code repository

Directory	Description
idhub_auth	User module where the users and the data encryption/ decryption system are defined.
idhub	The core directory of the IdHub project (templates, forms, views, models, etc.). It includes the main functionality of this Django project and the testing code.
locale	Contains localization files for IdHub (po and mo files for translations), enabling support for multiple languages. It's crucial for making the project accessible to a global audience.
oidc4vp	Module where all oidc4vp flows (implementation of the credential's presentation dialogue) reside.
promotion	Example module showing how to create a verifier portal that initializes the oidc4vp flow.
schemas	Module where the schemas reside for preload. These come from the schemas repository.
trustchain_idhub	The entry point of Django, where the global variables, the startup files and the file that defines the endpoints are defined.
utils	Different misc programs we developed. E.g. validation system for the Excel data loaded, SSIKit integration.
examples	Examples of different data files used in some functionalities.

The language used for this solution is Python, commonly associated with Django due to its Pythonic nature. Python's simplicity and readability make it ideal for web development, and the Django framework further enhances this with its robustness and flexibility.

The design pattern used here is the Model-Template-View (MVT) architecture, a variant of the traditional Model-View-Controller (MVC) pattern. In this pattern, the Model handles data and business logic, the Template deals with the presentation layer, and the View acts as the controller, connecting the Model and the Template (Shahdin, 2021).

The database used is SQLite, the default database for Django applications. However, Django can support other databases, such as PostgreSQL or MySQL, on a larger scale.

The application architecture consists of three parts: front-end, back-end, and database. The front end is what the user interacts with, implemented using HTML, CSS, and JavaScript. The back-end, implemented in Python using Django, handles server-side operations like processing user inputs, performing computations, and interacting with the database. The database stores and retrieves data as needed by the back end.

IdHub has three facets in a service instance for a given organisation: one for its admin or VC issuer, another for regular users of that organisation or VC holders, and another as a Verifier. An issuer would be responsible for uploading its own credible data for issuing specific data or credentials; a user wallet requests, holds, and presents user-related VC; and a verifier can validate VCs presented by third-party credential holders. These facets refer to different components within the application.

Verifier portals are built with tools from IdHub for verification and the OID4VP for the presentation dialogue. That combines with business logic and integration of the public portals of organisations offering services or benefits that allow subjects to apply for these by presenting credentials and acting as verifiers in the pilots. The *promotion* module shows how to create a portal that initialises the oidc4vp flow described below.

In general, the verification portal deals with these steps:

- Define a list of credentials that are able, willing or required to be verified.
- Establish a credential presentation/exchange dialogue with the holder.
- Verify the presented credential (presentation), store it securely, or process it, and proceed to the next page (either for authentication or submission to receive a benefit).
- Implement the different use cases of the demo.

Pre-conditions:

- There is a verifiability infrastructure to check details (identifiers for actors such as issuers and holders, based on DID and public keys),

optionally credentials from higher level organisations (TAO) that entitle trusted issuers (TI) to generate specific types of credentials.

- EBSI has a European scheme that adopts verifiable credentials as "verifiable attestations" with certain conventions. We follow them to align with it, and it relies on OIDC4VP.

3.5.2 Evaluation

We have deployed and evaluated IdHub through a set of use cases as pilots with communities that allow issuer and verifier organizations and subjects to access web services using decentralised authentication and verifiable credentials. These allow access to social benefits with accreditation of organisational membership, financial vulnerability, circular economy organisation, social and solidarity training, and federation membership.

3.5.3 Validation by testing

The basis for validation consists of passed manual and automated tests (CI) from the backend and frontend (UI) sides, combined with validation by a product owner actor in the project team and validation from user representatives from the participant organisations involved in each pilot. The solution is validated to work without any major issues (that could limit the intended operation) for the main end-to-end flow of each pilot. The software system (IdHub), including all related elements from DID identity generation, credential issuance, wallet and credential verification and post-processing, is operational and correct.

3.5.4 Validation by pilots

We concerted a set of pilots to cover diverse SSE cases. In terms of the set of deployed pilot testbeds for demonstration in Section 2, these are:

- Generic: with three service instances: 1. Generic: IdHub for demonstration on the stable branch; 2. Nightly: daily regenerated IdHub for stability testing of the development branch; 3. Autotest: regenerated IdHub pair at each commit for immediate testing and validation with the CI pipeline, including credential verification on a second IdHub instance.

- Open network "Nou Barris" district of Barcelona (xo9B): Vulnerable families in Barcelona's Nou Barris (9B) neighbourhood for fixed and mobile internet access. It involves the Pare Manel social work NGO working with families that assess their socio-economic situation and issue vulnerability credentials, the SomConnexió cooperative telecom provider, and the eXO.cat (part of guifi.net) community network as a verifier organisation providing reduced-cost internet access.
- LaFede: An NGO federation that provides training courses and services to other NGOs. They issued federation membership credentials, and under their request, we developed eIDAS1 (signed PDF) and eIDAS2 format credentials.
- Setem: Members of the Barcelona Setem NGO that is piloting offering benefits to members as (discounts from a fair trade online shop run by another regional Setem organization since Setem NGO is a federation.
- Pangea: access to Pangea services by members and beneficiaries of member organizations using their decentralized identity provider services.
- eReuse: Access to trusted/verifiable second-hand computer product information (inventory, datasheet) and information updates about product changes by certified circular economy actors.

Table 3 Pilots and roles of actors as issuer, holder, verifier.

Pilot	Issuer org.	Holder	Verifier org.
Generic	Demo issuer organizations	Individual demo holders	Demo verifier organizations
xo9B	Fundació Pare Manel (FPM)	Vulnerable families in the Nou Barris (9B) neigbourhood of Barcelona	(1) SomConnexió cooperative telecom provider, and (2) eXO. cat community network
Lafede	LaFede federation	LaFede member organizations	Third parties (not involved)
Setem	Setem Barcelona	Setem Catalunya association members	Setem Madrid
Pangea	eXO	eXO beneficiaries	Pangea
eReuse	Pangea, UPC	Refurbishers, recyclers, verifiers	UPC, Pangea

3.6 Discussion

In summary, the resulting experience and open-source software show the feasibility of creating an environment for trustworthy and reliable digital identities that help transition from paper-based, non-verifiable documents or eIDAS1 to eIDAS2 solutions, targeting identity and credential management for organisations engaged with activists and marginalised citizens (SSE sector).

The resulting system can be offered as software-as-a-service by Pangea and other equivalent organisations as infrastructure and service providers to other organisations and initiatives of this sector. The open-source model has great potential for replication, following a business model of functionality in exchange for a membership and a cost-oriented service fee (Burkett, 2012) (Burkett, 2020) (Lavinsky, 2023).

In terms of other impacts:

- Technological: Application and inclusion by offering secure decentralised digital identities to social and solidarity organisations (activists, marginalised citizens). This enhances trust and security in online interactions within the sector. The main benefit is that it simplifies processes in this sector by replacing paperwork with secure, verifiable digital information. This leads to smoother collaboration and reduced administrative burden.
- Socio-Economic Impact: Potential for economic growth, innovation, and job creation within the social and solidarity economy. Additionally, it fosters digital inclusion by providing secure access to online services.
- Environmental: While digital solutions have environmental drawbacks, they can also promote sustainability through energy efficiency and reduced physical waste (indirect benefits).

In terms of overall KPIs, usefulness and benefits, the most relevant contributions towards a more trustworthy and privacy-aware evolution of the internet are:

- Trust Assessment Effectiveness: Credential subjects work closely with support organisations, and subject trustworthiness is assessed by personal and documentation.

- Security guarantees on trustworthiness/privacy: We have integrated a verifiable data registry to record verifiable proofs of key actions (e.g. credential issuance).
- Security and privacy improvement: Disintermediation and automated verification (paperless) instead of paper-based or signed PDFs unsuitable for mass/automated issuance and verification.

Decentralization:

- Decentralisation: We designed and implemented multi-party interaction protocols to facilitate secure authentication and authorization processes between parties (e.g. OpenID Connect, OpenID for Verifiable Credentials)
- Decentralization improvement and user experience: It automates and integrates secure multiparty interactions using verifiable credentials not found previously in the SSE application domain.
- Scalability of the solution: We have limited results to assess its scalability as part of the pilots.

Sustainability business:

- Market penetration: For instance, in Spain, more than 50K social economy entities and more than 2 million jobs, 10% GDP and 12.5% employment. In the EU, about 3 million social economy enterprises and organisations.
- Profitability: Our model is cost-oriented as a commons infrastructure for the social and solidarity economy. The evident social benefits, spill-over effects, were not quantified.

Adoption:

- Task success rate: High to very high, but complexity affects more the less skilled participants.
- User adoption rate: Adoption is a lengthy process that has just started with the pilots, as all are new users.
- User satisfaction: High, as the service allows and facilitates otherwise unfeasible and inefficient manual accreditation, documentation and verification processes.
- User error rate: The pilots explore the feasibility and involve trial and error to polish functionality, with improvements in successive

software releases. We had two main software releases for the pilots to accommodate corrections and improvements to reduce room for mistakes.

- Time on task: Usage cycles are short per person involved, a few clicks for the issuance or presentation and automatic verification of credentials. Users were given specific instructions for their task in the context of each pilot.
- System Usability Scale: We had informal discussions with users that led to UI improvements during the testing and early piloting phase.

Pilot experiences:

- User Experience: We have had informal discussions with users that led to UI improvements during the testing and early piloting phase. Number of people involved in the qualitative research process: Around 25 people with different levels of involvement.
- User Engagement: On average 2-4 transactions, considering users managing and presenting credentials.
- Number of interested users in future business collaboration: Practically all organisations participating in pilots.
- User story (actions accomplished by users to complete the different use cases): Credential enablement, credential issuance, credential presentation, credential verification.

Innovation:

- Most disruptive technology components of your solution: A mechanism to generate verifiable credentials targeting eIDAS2 (not yet widespread, legally approved) that are legacy compatible with eIDAS1 (quite widespread, legally approved).

3.7 Related work

We discuss six system needs involving information management, purpose-driven credentials, settings with multiple organizations, and common information models for interoperability (W3VCWG) (W3CJS). Technologies like databases, encryption, web apps, and protocols such as SSO, ACL, OIDC, and VC are essential for functionalities like personal detail management, GDPR compliance,

role-based authorization, cross-organizational access, and secure authentication (OIDS)(OAUTH).

Standardization bodies like W3C, OpenID Foundation, and IETF are crucial in developing standards for verifiable credentials, OpenID, OAuth, and related technologies (W3VCD, 2022)(W3CDID, 2021)(OIDC). The Decentralized Identity Foundation (DIF) contributes to advancing decentralized identity technologies (DIF).

Relevant standards include W3C Verifiable Credentials, OpenID Connect (OIDC), and the EBSI ID model, which uses blockchain for decentralized identity management (EBSI). Regulatory frameworks like GDPR and eIDAS impact how these technologies are implemented, emphasizing data protection and secure electronic transactions (GDPR, 2016)(EIDAS, 2014).

Technologies for authentication, authorization, and identity management have evolved from LDAP to modern solutions like OpenID Connect, SSO, CAS, LDAP, SAML, and SCIM (OIDC)(WSSO)(WLDAP)(WSCIM)(SCIM, 2020). Open-source identity providers like Keycloak, LemonLDAP::NG, Authelia, and Authentik offer various functionalities for identity and access management (TOR, 2023).

For verifiable credentials, solutions like Veramo, SpruceID, Walt.id provide VC issuance, verification, and wallet functionalities. Our prototype implementation uses SpruceID's open-source solutions, leveraging the IOTA stable network and the IOTA-EBSI testbed for VC and VP support (IOTA)(EBSI) as well as a verifiable registry we implemented using a permissioned Ethereum ledger.

Identity services can utilize IOTA identity services or the IOTA-EBSI variant, with client libraries for operational use IOTA Identity Services. The IOTA Identity Services, built on the Tangle, integrate with SpruceID SSI infrastructure, offering a framework for creating and managing decentralized identities (IOTA)(SSI, 2021).

3.8 Conclusion

The research project has successfully developed and deployed a decentralized digital identity and credential management system, IdHub, tailored for organisations working with activists and

marginalised citizens. This system has defined a sample set of schemas for the social and solidarity economy. It includes modules for issuer, holder, and verifier roles and auxiliary modules for authentication and access control. The software has been implemented in a suitable platform and deployed in the infrastructure platform, with validation through pilot experiences with relevant communities.

The key achievements include the public release of the software code implementation, developing a social business model and exploitation plan to understand the feasibility for a community and an infrastructure service provider, and the lessons learned from pilot activities with user communities. The system supports pilot experiences with representative communities of the target sector. The project has also demonstrated the potential for replication.

Since credentials are cryptographically signed and can be verified without involving a central authority, users can share specific pieces of information while maintaining control over their data and privacy. Together, DIDs and VCs allow users to take ownership of their digital presence, fostering a decentralized, trust-based web where peer-to-peer interactions are prioritized, reducing reliance on centralized data and enhancing security.

However, DIDs and VCs come with several risks. These include the complexity of implementation, which may slow adoption. The lack of central oversight makes dispute resolution and governance challenging. Privacy and security issues can arise from poor key management, while reputation attacks may occur if a DID is compromised. Interoperability issues between different systems could lead to fragmentation, and reliance on blockchain infrastructure presents scalability and regulatory concerns.

Potential future developments or improvements include iterating to improve the solution based on user engagement plan insights, which involve adjustments and changes in the product or service, improving the user experience, or adjusting offering and recruitment strategies. Pangea.org offers an experimental service for their member organisations, open for third-party organisations to do the same as part of an open community of developers and users. The team in Pangea and UPC continue to monitor and evaluate the

solution's effectiveness, making necessary adjustments to streamline the business and exploitation plan. The ultimate goal is to ensure that the solution meets users' needs, provides a positive user experience, and can become self-sustaining, operating in the context of eIDAS2 and EBSI to include the social and solidarity sector in a digital Europe.

3.9 References

(Borzaga, 2019) Borzaga, C., Salvatori, G., Bodini, R. (2019). *Social and Solidarity Economy and the Future of Work*. Journal of Entrepreneurship and Innovation in Emerging Economies. https://doi.org/10.1177/2393957518815300.

(Burkett, 2012) Burkett, I. (2012). An introduction to co-design. Sydney: Knode, 12. https://www.yacwa.org.au/wp-content/uploads/2016/09/An-Introduction-to-Co-Design-by-Ingrid-Burkett.pdf.

(Burkett, 2020) Burkett, I. (2020) Using the Business Model Canvas for Social Enterprise Design, 2nd Edition, The Yunus Centre. https://www.griffith.edu.au/__data/assets/pdf_file/0037/997156/BMC-for-SE-2nd-Edition-Web.pdf.

(DeviceHub) DeviceHub service. Retrieved from https://github.com/eReuse/devicehub-teal.

(DIF) Decentralized Identity Foundation, https://identity.foundation.

(EBSI) European Commission. (n.d.). European Blockchain Services Infrastructure (EBSI). Retrieved from https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/About+us.

(EBSI, 2024) European Commission (2024). Introducing EBSI. Retrieved from https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home.

(EBSIID, 2021) European Commission. (2021). EBSI Identity. Retrieved from https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Homepage.

(EBSIUC, 2023) European Blockchain Services Infrastructure (EBSI), Use Case families and domains (2023). Retrieved from https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi.

(EIDAS, 2014) European Union. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union, L 257, 73-114. Retrieved from https://eur-lex.europa.eu/eli/reg/2014/910/oj.

(EIDAS, 2024) European Union. (2024). European Parliament legislative resolution of 29 February 2024 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)) Retrieved from https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.html.

(EP, 2022) European Parliament. (2022). Revision of the eIDAS Regulation: findings on its implementation and application (Briefing). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf.

(ESS, 2019) European Union. (2019). European Self-Sovereign Identity Framework (ESSIF) . Retrieved from https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about.

(GAT, 2021) Gataca, The impact of the new eIDAS proposal on the SSI community. Retrieved from https://gataca.io/blog/here-s-what-the-new-eidas-proposal-really-means-for-the-ssi-community-in-6-key-points/.

(GDPR, 2016) European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

(IOTA) The IOTA Tangle, identity and verifiable credentials https://docs.walt.id/v/ssikit/ecosystems/iota.

(ITUX, 2021) International Telecommunication Union. (2021). X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (Corrigendum 1). Retrieved from https://www.itu.int/rec/T-REC-X.509-202110-I!Cor1/en.

(Lavinsky, 2023) Dave Lavinsky, Growthink (2023). Social Enterprise Business Plan Template, https://www.growthink.com/businessplan/help-center/social-enterprise-business-plan.

(MUS) Musician, https://gitlab.pangea.org/santiago/django-musician.

(OAUTH) IETF Working Group Web Authorization Protocol (oauth). Retrieved from https://datatracker.ietf.org/wg/oauth/about/.

(OID4VP) Terbu, O., Lodderstedt, T., Yasuda, K., Lemmon, A., and T. Looker. (2021). OpenID for Verifiable Presentations. Retrieved from https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

(OIDC) OpenID, What is OpenID Connect. Retrieved from https://openid.net/developers/how-connect-works/.

(OIDS) OpenID, What are OpenID Specifications. Retrieved from https://openid.net/developers/specs/.

(ORCH) Orchestra. Retrieved from https://gitlab.pangea.org/dcastro/django-orchestra https://github.com/glic3rinu/django-orchestra/.

(PRO, 2023) Propel non-profits (2023). Social Enterprise Business Plan, https://propelnonprofits.org/resources/social-enterprise-business-plan/.

(Sabiescu, 2013) David, S., Sabiescu, A. G., Cantoni, L. (2013, November). Co-design with communities. A reflection on the literature. In Proceedings of the 7th International Development Informatics Association Conference (No. 2013, pp. 152-166). Pretoria, South Africa: IDIA..

(SCIM, 2020) IETF. (2020). SCIM 2.0 Protocol Specification. Retrieved from https://datatracker.ietf.org/doc/rfc7643/.

(Shadhin, 2021) Shadhin, F. (2021). The MVT Design Pattern of Django. Python in Plain English. Retrieved from https://python.plainenglish.io/the-mvt-design-pattern-of-django-8fd47c61f582.

(SIOP, 2023) OpenID Connect (2023). Self-Issued OpenID Provider v2, Retrieved from https://openid.net/specs/openid-connect-self-issued-v2-1_0.html.

(SSI, 2021) World Economic Forum. (2021). Self-sovereign identity: The future of personal data ownership? Retrieved from https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/.

(TOR, 2023) TOR (2023). TOR System and Service Administration Projects. Retrieved from https://gitlab.torproject.org/tpo/tpa/team/-/wikis/howto/ldap#single-sign-on.

(VR, 2023) UPC Distributed Systems Group (2023). UPC verifiable registry. Retrieved from https://gitlab.com/dsg-upc/ereuse-dpp.

(W3CDID, 2021) Sporny, M., Guy, A., Sabadello, M., and D. Reed, Decentralized Identifiers (DIDs) v1.0, 2021. Retrieved from https://www.w3.org/TR/2021/PR-did-core-20210803/.

(W3CJS) W3C JSON for linking data community group, (n.d.). JSON-LD (JavaScript Object Notation for Linking Data) Retrieved from https://www.w3.org/community/json-ld/.

(W3CVC, 2019) www.w3.org, (2019). Verifiable Credentials Data Model 1.0. Retrieved from https://www.w3.org/TR/vc-data-model/.

(W3VCD, 2022) W3C. (2022). Verifiable Credentials Data Model 1.0. Retrieved from https://www.w3.org/TR/vc-data-model/.

(W3VCWG) W3C Verifiable Credentials Working Group. (n.d.). W3C Verifiable Credentials Working Group Test Suite. Retrieved from https://w3c.github.io/vc-test-suite/.

(WLDAP) Wikipedia (n.d.). LDAP - Lightweight Directory Access Protocol. Retrieved from https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol.

(WSCIM) Wikipedia (n.d.). System for Cross-domain Identity Management (SCIM). Retrieved from https://en.wikipedia.org/wiki/System_for_Cross-domain_Identity_Management.

(WSSO) Wikipedia (n.d.). Single sign-on. Retrieved from https://en.wikipedia.org/wiki/Single_sign-on.

4 Cyber Security Essentials for a Community Internet Network in India: Strategies for Management and Mitigation

Osama Manzar and Suruchi Kumari

Abstract

Cyber Security of community internet networks remains a challenge, especially in low-income communities. We explore the critical dimensions of privacy and cybersecurity from socio-behavioural, legal and technical aspects. In the wake of the evolving regulatory legal ecosystem of data privacy, data protection and standardisation of information handling, it becomes the duty of the organisation/service provider to ensure continuous compliance. This also paves the way for a much-needed focus on cyber security at the service level. The essentials of establishing a secure Community Network follow the fundamental principles and practices required to secure a local or regional network. It requires an all-encompassing approach that includes social awareness about personal/user data protection, secure network infrastructure, regulatory compliance, user awareness, security operator training, and collaboration. Implementing these cybersecurity essentials would enable the community networks to provide safe and reliable internet access while minimising potential cyber risks.

4.1 Introduction

We live in a world where the physical and digital unavoidably intertwine in an individual's daily life in multiple ways. The digital infrastructure has made daily utilities simple and swift, from socialisation to finance management and accessing private and public services. Notwithstanding the disparities in accessibility to digital services and infrastructure between the urban and the rural, the digital aspects of life have made their footprints clear. Together with the evolving aspects of neural networks in Artificial Intelligence, Machine Learning and cloud computing innovations, the world is becoming increasingly data-driven, and information is becoming a

vital commodity that is highly valued. There is no contention that the technology and services stakeholders are eager to accumulate dynamic data on individuals. On the other hand, individuals are also non-hesitant in entrusting digital platforms with their details for availing online services. The gap between the idea of privacy and the sense of privacy is widening and turning virtual. This changing nature of the Internet as a commodity rather than a service for the citizens is bringing out various challenges in Internet governance.

In this essay, we try to understand the multiple dimensions of privacy and cyber security, focusing on community-level Internet networks. This is explicitly wanted as, unlike at the individual level, there is less choice, autonomy, and awareness of addressing issues arising from information privacy and secure communication privacy when it comes to community-based Internet networks.

4.2 Community Internet Networks Now

Over the last decade, the international community has recognised the need to advocate for Community Networks or Community based Internet Networks. Over the years, the Dynamic Coalition on Community Connectivity[21] has focused on different aspects of Community Networks ranging from Sustainable Funding Models, governance, benefits, challenges, policy gaps and others (2021,2019, 2017). Now, the time has come to talk about the privacy and cybersecurity of Community-oriented Networks. Despite the challenges around CNs, particularly in developing countries like India, a small but firmly committed civil society organisation like Digital Empowerment Foundation (DEF) is working towards making CNs functional, meaningful, and secure for vulnerable populations isolated from the benefits of digital integration.

In India till 2016, CNs lacked a proper definition in common parlance or government's ICT policy or regulations (Srivastava,2017). The Consultation Paper on 'The Proliferation of Broadband through Public Wi-Fi Networks' by the Telecom Regulatory Authority of India

21 The Dynamic Coalition on Community Connectivity (DC3) is a multistakeholder group established under the auspices of the United Nations Internet Governance Forum (IGF), dedicated to promoting the discussion on community networks (CNs). DC3 furthers analysis of how CNs may help create sustainable Internet connectivity while empowering Internet users.

(TRAI) identified CN as "public Wi-Fi networks". While assigning a broader meaning to CN did not restrict it to merely a Wi-Fi hotspot by telecommunications service providers (TSPs)/ ISPs in public places, instead it also recognised small entrepreneurs or private entities who could sell Wi-Fi network services for public use (Srivastava, 2017). DEF has more than 280 locations under their targeted program called W4C (Wireless for Communities)[22] spread across India. Since then, CN has been adopted by DEF as a concept and a frugal methodology to enable last-mile access for the marginalised and unreached communities living in telecom dark areas lacking meaningful access. W4C has been intelligently using 2.4 Ghz and 5.8Ghz unlicensed spectrum and simple methodologies of community networks like point-to-point, point-to-multipoint, and mesh networking, using backhauls from any of the telcos, including public sector telcos. In the last 15 years, W4C has reached more than 2000 villages, covered more than a million households and spread across 250 districts in about 15 states of India.

Over the years, establishing CNs has shown emerging issues for community development. CNs' public nature has brought privacy and cybersecurity issues to the centre. In the following sections, we will discuss the meaning of privacy in Indian society, the legal and regulatory frameworks around privacy and cybersecurity, and the challenges of securing cybersecurity in community networks and finally, discussing the best practices adopted by Digital Empowerment Foundation for securing privacy and cybersecurity for Community Networks in India.

4.3 Privacy and Indian Society

The idea of privacy is multidimensional. This cannot be explained with a single definition, and the concept has broad historical roots with different explanations in the legal, philosophical, and political discourses. It could mean concealment of information, peace, or freedom and autonomy per the use instance. In information systems, privacy is now considered a commodity that could be exchanged for

22 However, regarding the number of exclusive Community Networks, DEF's W4C has a reach of up to 170 plus. The W4C program of DEF was started in 2010 with exceptional support from the Internet Society.

perceived net benefits. For the benefit of this essay, let us understand privacy as the ability of the individual to control the terms under which their personal information is collected and used.

It is a fact that ancient societies did not formally acknowledge the concept of privacy, and the concept evolved with the progress of human civilisation, and individual rights became important only at the advent of industrial society. In the legal discourse, the first mention of individual rights can be traced back to the promulgation of the Magna Carta in 1215 CE, which introduced the basic idea of defined rights and liberties for everyone. Gradually, in the last century, when cultures grew in complexity with techno-industrial and post-industrial developments that they could not resist, privacy became an integral part of our moral system, and legal systems had to be put in place to protect individual privacy. However, the social structure in India, founded on community morale, has less space for non-private community life even now. In his work, *Privacy 3.0: Unlocking our Data-Driven Future,* Matthan (2018) explains the trajectory of the evolution of the concept of privacy over the years after the independence of India. He draws a vivid picture of how non-privacy was a fundamental need rooted in survival, how it anthropologically evolved with the rise of private spaces and individual thought, and how technology is invading private spaces and thoughts. In the trajectory of his arguments, this work points to the deep-rooted connection that the sense of 'safety and wellbeing' has with the non-private life existing in the Indian social psyche.

Lacity and Coon (2024), in their book 'Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives' calls privacy a 'wicked problem' in the modern context as this concept refers to a socially complex problem involving multiple stakeholders with differing perceptions and preferences, and levels of power. It is also intriguing to understand the slippery slopes in the concept when the virtual and physical worlds coexist and overlap in daily lives.

A face-to-face conversation in the physical world that is digitally recorded with or without the knowledge or consent of the actors in it, getting stored or disseminated in the virtual world, which the innate actors have no control over, has imminent threats and might be against the perceived notions of privacy for them. The feed of

a privately owned closed-circuit camera focused on public spaces has no concern over the privacy of individuals who utilise the public space. This physical-digital intertwining has become more and more layered and complex with shared technologies such as cloud servers and networks of connected technologies. In India, Privacy as a part of Cybersecurity is a socio-behavioural challenge where DEF has been working by spreading awareness and training about the meaning of privacy and its need in ordinary people's language so that they can be part of the digital ecosystem as dignified citizens rather than mere consumers of the Internet infrastructure.

4.4 Privacy and Legal Frameworks

The 'privacy' debate has had its legal interventions in the last decade with government interventions such as the General Data Protection Regulation (GDPR) of 2016 in Europe, California Consumer Privacy Act (CCPA) of 2018 in the US, General Data Protection Law (LGPD) of 2019 in Brazil, Protection of Personal Information Act (POPIA) of 2020 in South Africa, the PRC Personal Information Protection Law (PIPL) of 2021 in China, and the Digital Personal Data Protection Act (DPDPA) of 2023 in India. All these regulations aim to protect the subjects' personal information, rights, and interests, standardise personal information handling activities, and promote the rational use of personal information.

The Supreme Court of India in Justice *K.S. Puttaswamy and Anr. v. Union of India and Ors* landmark judgement declared that 'the right to privacy is part of the fundamental right to life in India' and that the right to informational privacy is part of this right. Considering the broad frameworks of the national and international regulations and the active presence of authorities such as the Data Protection Authority in India, it is highly important to consider the known and unknown flow of personal information in the physical and cyber realm.

4.5 Community Internet Networks and Cybersecurity: Common Challenges

Community Networks serves as the not-for-profit way of enabling accessibility and building the digital divide through tailored solutions at the local level for a small rural/remote community. It is typically a

decentralised, locally controlled infrastructure to provide affordable/free internet access to underserved communities. As envisaged and suggested, it does not attract high investments in installation and maintenance. It is a solution to bridging the internet gap by connecting the unconnected, enabling them to access education, work, and each other.

These systems leverage networks of connected technologies to provide more efficient, innovative, affordable, and manageable infrastructure locally. It is a sustainable concept with optimum choice for the communities to choose what is best for their needs. It is pertinent that a greater scale of awareness of technology is required for any community network to function. Given the high internet dependency, ensuring these networks' security is essential to protect user data, maintain service integrity, and prevent malicious activities. Additional technical expertise would be required to ensure the safety, security and privacy of data flow on the network. This is seldom a concern with community networks as it demands better financial allocations and dynamic monitoring, which would be unlikely.

At the implementational level, small-scale community networks face quadruple trouble regarding adequate financing, management and maintenance, expert availability, and awareness, compromising user security. Community Networks work on a limited budget, restricting the purchase of advanced hardware and security tools. It also results in higher long-term expenses and low maintenance. Due to their remote locations and low profitability, these networks struggle in terms of management and maintenance, which are mandatory for ensuring uninterrupted service. The unavailability of experts to configure the hardware used in the network who could continue to provide the same scale of service is another trouble. The most crucial issue, undoubtedly, would be the lack of awareness of individual users regarding privacy and cyber security. This makes it easier for cyber threats such as spamming, phishing, piggybacking or baiting to occur to the individual and, at times, to all the devices on the network.

4.6 Data Privacy, Cybersecurity and Cyber Capacity in CNs

In the wake of the evolving regulatory legal ecosystem of data privacy, data protection and standardisation of information handling, it becomes the duty of the organisation/service provider to ensure continuous compliance. This also paves the way for a much-needed focus on cyber security at the service level.

In the information security and data security realm, DEF is working towards the fundamental of data privacy, following the security management protocol of ISO/IEC 27000 family[23] could be the foundational step. All the hardware, software, and services must comply with the Information Security Management Standards (ISMS) of ISO27K and must be mandated beforehand to design and implement a Community Network. This would also bolster cybersecurity as online security threats intensify.

An additional step of having a physical firewall at the hardware level between the Private Local Area Network/Community Network and the Internet is to be ensured. This would help devise a default rule for all the network devices and devices connected in the future while also saving the system's processing power by not requiring the software-level network traffic analysis. It could also kill the blind spots and safeguard the network from targeted attacks.

The next level is to have hardware in the Community Network with built-in firewalls and customise the rules accordingly. Cost-effective MikroTik CCR1036[24], RB1100AHx4[25], and RB3011UiAS[26] routers and

23 The ISO/IEC 27000 Information Technology Security Techniques Collection provides the requirements, vocabulary, code of practice and risk management techniques to implement and establish an effective IT security management system. It also guides auditing and certifying an information security management system.

24 CCR1036-12G-4S (Cloud Core Router)is an industrial-grade router with a cutting-edge 36-core CPU. It provides many millions of packets per second. The device comes in a 1U rackmount case and has four SFP ports, twelve Gigabit ethernet ports, a serial console cable and a USB port.

25 RB1100AHx4, 13x Gigabit Ethernet ports Router, powered by AL21400 CPU with four Cortex A15 cores, clocked at 1.4GHz each, for a maximum throughput of up to 7.5Gbit. The device supports IPsec hardware acceleration (up to 2.2Gbps with AES128).

26 RB3011 is a new multi-port device, running an ARM architecture CPU for higher performance than ever before. The RB3011 has ten Gigabit ports divided in two switch groups, an SFP cage and for the first time a SuperSpeed full size USB 3.0 port, for adding storage or an external 3G/4G modem. RB3011UiAS-RM Unit comes with 1U rackmount enclosure, a touchscreen LCD panel, a serial console port and PoE output functionality on the last Ethernet port.

ports are part of the core router boards for establishing point-to-point or point-to-multipoint devices such as Base box, LHG[27], and SXT[28] to achieve this objective. These devices are globally tested, trusted and devoid of backdoors.

Ensuring that the operating systems at the Community Network management level and the user level have trusted and updated versions of the antivirus and anti-malware software installed and that regular scans are scheduled could do wonders in mitigating and managing cyber threats. Open-source log management protocols such as syslog-ng can add to the anti-virus protection as it helps content-based filtering. The intrusion detection and prevention system and DDoS[29] protection may be integrated to prevent hacking attempts and DoS attacks.

End-to-end encryption of sensitive data, minimising data collection, multi-factor authentication and strong password policies for all users, authorised access and role-based access control, redundant systems for backup and failure support, open-source audited solutions, and data localisation are additional (optional) steps that may be utilised to further foolproof and strengthen the security of the Community Network.

4.7 Conclusion

As a stakeholder-own and operated service, the Community Networks assumes that dynamic management occurs at the root level. This includes training and generating experts within and continuously educating the beneficiaries through awareness campaigns on data privacy and digital well-being. It envisages a shared knowledge system to be generated within.

Risk mitigation training programmes and modules must be devised for this. This should be a comprehensive guideline to safe practices

27 Light Head Grid (LHG) is a compact and light 2.4 GHz 802.11b/g/n wireless device with an integrated dual polarization 18 dBi grid antenna at an affordable price. It is perfect for point-to-point links or for use as a CPE at longer distances and supports Nv2 TDMA protocol.

28 SXT Lite5 is a low cost, high transmit power 5GHz outdoor wireless device. It can be used for point-to-point links or as a CPE for point-to-multipoint installations.

29 DDoS (distributed denial-of-service) protection is a security solution that detects and defends against DDoS attacks. DDoS attacks can quickly ramp up, so effective protection requires real-time traffic analysis and a prompt response.

that teaches the users what is not to be done on the internet. This may include practices such as a) recognising genuine websites and internet frauds, b) safe surfing and identifying common cyber threats, c) privacy and security of the passwords and online accounts, d) regular cybersecurity analysis and attack prevention, and e) hands-on-training of commonly used hardware (smartphones, routers, modems) and software (antivirus, firewalls).

The essentials of establishing a secure Community Network follow the fundamental principles and practices required to secure a local or regional network. It requires an all-encompassing approach that includes social awareness about personal/user data protection, secure network infrastructure, regulatory compliance, user awareness, security operator training, and collaboration. Implementing these cybersecurity essentials would enable the community networks to provide safe and reliable internet access while minimising potential cyber risks.

4.8 References

Alam, S. & Manzar, O. (2019). Community Network and Democratising Access: Addressing the Question of Sustainability in Belli, L. & Hadzic, S. (Eds). (2021). *Community networks: towards sustainable funding models Official Outcome of the IGF Dynamic coalition on Community Connectivity*. conconnectivity.org; FGV Direito Rio. https://comconnectivity.org/wp-content/uploads/2021/12/Community-Networks-Towards-Sustainable-Funding-Models.pdf.

Belli, L. & Hadzic,S. (Eds).(2021). *Community networks: towards sustainable funding models Official Outcome of the IGF Dynamic coalition on Community Connectivity*. conconnectivity.org; FGV Direito Rio. https://comconnectivity.org/wp-content/uploads/2021/12/Community-Networks-Towards-Sustainable-Funding-Models.pdf.

Belli, L. (Ed.) (2017). Community Networks: the Internet by the People, for the People Official outcome of the UN IGF Dynamic Coalition on Community Connectivity. conconnectivity.org FGV Direito Rio. https://comconnectivity.org/wp-content/uploads/2020/05/community_networks_-_the_internet_by_the_people_for_the_people.pdf.

Belli, L. (Ed.) (2019). Building Community Network Policies: A Collaborative Governance towards Enabling Frameworks Official Outcome of the IGF Dynamic coalition on Community Connectivity. FGV Direito Rio. https://comconnectivity.org/wp-content/uploads/2020/05/building_community_network_policies_-_a_collaborative_governance_towards_enabling_frameworks.pdf.

K. S. Puttaswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India Aug. 24, 2017).

Lacity, M. C., & Coon, L. (2024). Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives. Springer Nature.

Manzar, O. (2016). Public WI-FI hotspots can be new PCO booths. The Mint.

Matthan, R. (2018). Privacy 3.0: Unlocking Our Data-Driven Future. HarperCollins.

Srivastava, R. (2017). Community Networks: Regulatory issues and gaps – Experiences from India. Digital Empowerment Foundation.

Treguer,F & Rosnary,M.D (2019). Telecommunications Reclaimed: A Hands-On Guide to Networking Communities. ISOC.

5 Localised community networks co-create the internet with information security and cultural ethics: A Case Study from India

Ritu Srivastava

Abstract

The proverb 'all roads were supposed to lead to Rome' is now changed to 'information is highway' and leads Rome right to our home. In today's world, anyone can travel to Rome virtually through its internet-enabled handheld device, but how many of them understood the power of internet. India is chasing the dream of digital Bharat by crossing the internet penetration rate to 52% and became the second highest in active internet users after China. However, data shows that 56 per 100 inhabitants have a mobile broadband subscription, versus only 2 per 100 connecting to the internet via a fixed broadband subscription. Giants like Reliance Jio and Airtel occupy over 90% market share, yet over 25000 villages in India lack mobile and internet connectivity[30]. This digital divide impacts every aspects of life, including digital healthcare, financial, education and economic opportunities.

Community Networks (CNs) are such local telecommunication infrastructures that are built, managed and operated by local communities serving the rural and unconnected population who can't afford traditional connectivity services or solutions. Having a multi-stakeholder approach, these network use variety of open source tools and unlicensed spectrum to provide affordable connectivity and other support services for improving the lives of rural and unconnected communities socially and economically. Partnering with local entities and having decentralized network approach for sustenance makes it unique in comparison to traditional ISPs.

30 Economic Times, How India is using the Internet https://economictimes.indiatimes.com/tech/technology/how-india-is-using-the-internet/articleshow/108354854.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

Jadeite's CR Bolo, is one such example that enables community radio station (Radio Bulbul) to explore the opportunities of connectivity and provide ubiquitous and meaningful connectivity in neighbourhood communities of Bhadrak district. The paper focuses on decentralization model of connectivity that is helping in preserving culture ethics and enabling communities to co-create the internet together.

5.1 Introduction

Globally, there are around 2.6 billion people do not have access to the internet, according to a 2023 study by the International Telecommunication Union (ITU)[31]. This means that 3% population in the world is unconnected. The existing and ongoing digital exclusion deprives a generation with the opportunity to develop their potential and ability to uplift their entire communities.

Connecting the unconnected population in both rural and urban areas to connect with the internet presents an important challenge for development practitioners and policy makers[32]. There are many reasons such as poverty, lack of reliable service, access to linguistically and culturally relevant content, access to equipment and training and, access to network infrastructure. The COVID pandemic has exposed the existing inequalities in internet access and lack of information availability across the globe. Equitable access to public services (including health care and education) and information cannot be delivered without having equitable broadband access services.

Most importantly maintaining privacy and preserving cultural ethics of locals is challenging for policy makers and development practitioners. Conventional commercial telecommunication networks models are able to provide access to the internet services however, not able to address other access-related challenges such as provision of digital literacy to locals, preserving cultural ethics and local content.

31 Population of global offline continues steady decline to 2.6 billion people in 2023, ITU Press Release, https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx.

32 USAID and the Digital Impact Alliance (2017) Closing the access gap: Innovation to accelerate universal Internet adoption, https://2017-2020.usaid.gov/sites/default/files/documents/15396/Closing-the-Access-Gap.pdf.

One way communities are overcoming network access barriers by creating network themselves. A network architecture built and operated by the people as a collaborative response to manage their own services, ability to develop their own content and manage and operate their network.

Community networks are one of the most promising solutions that are bridging the digital divide and information access barriers in rural and underserved areas of global south countries. By definition, community network are crowdsourced networks primarily built by citizens or non-profit organizations[33]. These networks are decentralized and autonomous networks that establish or augment internet and connectivity services where internet connectivity is either not available or scarcely available[34]. These community networks are established at community-owned spaces primarily managed by local organizations or local leaders. These spaces are used for setting up the local server, uploading and managing the content, functioning as metropolitan intranets and enabling access to digital services for communities.

Jadeite Solution is one of the similar organization that has made its effort to bring a community network model in disadvantaged and digitally excluded areas through local partnership with Community Radio station – Radio Bulbul located in rural Bhadrak district of Orissa. CR Bolo, operated and managed by Radio Bulbul is one of the community networks in rural Orissa that is not only bridging the digital divide but also enabling communities to create an inclusive and culturally diverse internet locally. This paper brings the case study of CR Bolo community network that focuses on the concept of right to co-create the internet and preserve the local content and ethics. The paper also share some experiences that give us perspective on the future of community-driven connectivity as a fundamental enabler to the right to co-create the internet.

33 P. Micholia et al., "Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3581-3606, Fourth quarter 2018, doi: 10.1109/COMST.2018.2817686.

34 Upasana, Community networks: states, solutions and communities, GenderIT.org, https://genderit.org/feminist-talk/community-networks-states-solutions-and-communities.

5.2 Community network: Decentralized model for internet connectivity

Conventionally, government and private stakeholders are held to be responsible for providing the connectivity services in any country be it setting up mobile or network towers or laying out optic fibre reaching to remotest parts of their respective country. However, digital infrastructure including access to backhaul connectivity, network towers and backbone optical fibre is yet largely absent in rural regions of the world. Traditional telecom models of broadband and mobile connectivity have failed to connect rural regions because the return on investment in such places is insufficient[35]. Digital technologies and network architecture are embedded in structures and systems of power, with mainstream technologies and policies that are developed in institutions and knowledge paradigms, far removed from those people whom need to be connected and seek to improve. Moreover, the digital connectivity and its related services are primarily not available for marginalised communities because of systematic barriers including affordability, access to digital skills and education, language and literacy obstacles and also perceived relevance and social norms. The design of such traditional architectures are often centralized and underpinned by concepts that are not applicable for people living in marginalised communities or located in remotest villages. These networks are often not designed as per local needs and wholly unaccountable to community governance and local knowledge.

There are numerous studies that have explored the concept of bottom-up approaches for connectivity that challenge the androcentric, expensive top-down approaches adopted by mainstream ISPs. Addressing gaps in connectivity infrastructure, left by the state and private bodies, community-owned and operated networks, also known as community networks (CNs) play an important role in providing the last mile connectivity. Framed as an infrastructural solution, these community networks are focused on the specific need of community and bring decentralized network and decolonised technology that don't follow such hierarchical systems, infrastructure and governance models. The design of community network is beyond

35 Bhattacharjee 2021; Community networks: states, solutions and communities; https://genderit.org/feminist-talk/community-networks-states-solutions-and-communities.

the concept of connectivity, it seeks to explore the opportunities around meaningful connectivity which is easily accessible, affordable and have collaborative effort[36]. It allows people to access information freely, able to access unbiased internet services, seek their well-being express themselves and create content while also actively engaging in development discourses[37]. The community networks are emerged as a participatory innovative model for delivering meaningful internet connectivity to the regions where traditional ISPs are not able to reach and provide the connectivity.

This is what makes community network unique and different from traditional ISPs. People are at the centre of any community network development since the infrastructure is built, managed, operated and administered by community-driven organization or by group of people by pooling their existing resources and making collaborative effort for building infrastructure [38,39]. Srivastava (2017a, 2017b:15) highlights that community networks works with local partners to start-up and scale up their activities. Moreover, the diversity of stakeholders and social groups across communities invites further work to unpack the roles played by different social stakeholders and groups. Schuler (1994:41) study identifies that values and attitudes – the politics of community network makes participation in community network development important[40].

Each community network offer variety of services and adopt different sustainability approaches as per the need of their community[41]. These services can be grouped as given in below figure in a bundle and provided in a community driven approach.

---

36 A4AI. (2020). Meaningful Connectivity: A New Target to Raise the Bar for Internet Access. Alliance for Affordable Internet. https://docs.google.com/document/d/1qydsmTY4hln3pP4dWJbCSRFna8SfDYAtGfacKYwhVk8/edit).

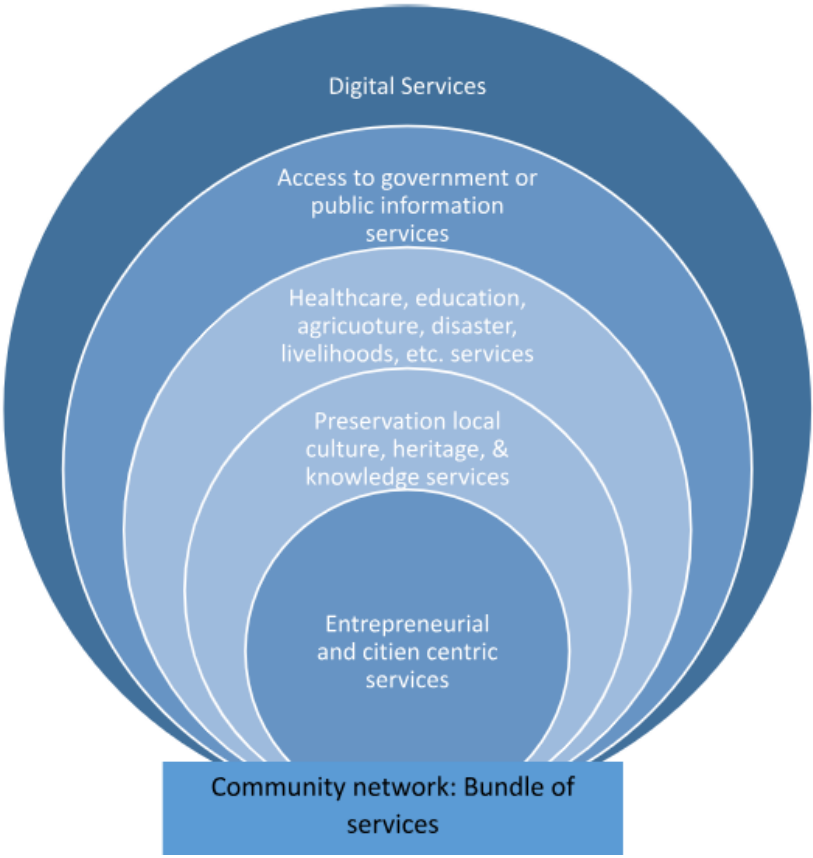
37 Best Practices Forum, Gender and Access (2018) https://www.intgovforum.org/multilingual/content/bpf-gender-and-access-2018.

38 Srivastava R (2017a) Community networks: regulatory issues and gaps – experiences from India. Available at https://www.internetsociety.org/resources/doc/2017/community-networks-regulatory-issues-gaps-experiences-india.

39 Srivastava R (2017b) Policy gaps and regulatory issues in the Indian experience on community networks. In: Belli L (ed) Community Networks: The Internet by the People, for the People: Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, pp. 153–192.

40 Schuler D (1994) Community networks: Building a new participatory medium. Communications of the ACM 37(1): 38–51.

41 Srivastava R (2021); Fostering Global and Local Community Radio Partnerships for Community Network Development: A Case-Study from India; Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity Towards Sustainable Funding Models.



In multi-stakeholder partnerships approach, people bring different skills and abilities for setting up a community network. Often, these partnerships amongst local organisations are for knowledge sharing that are built on trust and between non-hierarchical members whose participation is voluntary (Solan, 2013)[42]. Local people share their knowledge, resources and learnings about the culture and heritage that are mostly developed in local dialect or language. Sharing information is a critical aspect for development of any community and the foundation of establishing any community network.

42 Sloan, P., and Oliver, D (2013). Building Trust in Multi-stakeholder Partnerships: Critical Emotional Incidents and Practices of Engagement. In Organisational Studies 34 (12), p1835-1868.

Evolution of the network and the internet, threats to information and networks have also risen dramatically. Most of these threats are cleverly exercised attacks causing damage or committing theft. As personal information is becoming more prevalent on the internet, there are many security risks to individuals. Network security is one of the key component in information security because it is responsible for securing all information passed through networked access points[43,44]. Securing the network refers to hardware and software functions, characteristics, features, operational procedures, accountability measures, access controls, administrative and management policy required to provide acceptable level of protection for hardware, software and information in a network.

In a multi-stakeholder approach, when the community networks are co-created and designed, these networks understand the concept of information security of the locals. Conceptually, these community networks are designed from bottom-up approach, they are thoughtful about maintaining local's security, preserving local culture and knowledge. Because building, operating and using a community network involve more than just the technical aspects of telecommunications, benefits extend deep into the fabric of local society. Unlike traditional networks, community networks provide the localised communication channels that people can use them as per their requirements. In result, it also means they are not accessing internet services 24*7, however, localised communication platform give them opportunity to be interconnected. Community networks have also played a vital role to bridge different parts of society such as between newcomers and migrants, supported people's cultural identity, improved local security and safety; provoked and informed local discussion about privacy, and supported intergenerational cooperation[45].

43 Chen S., Iyer R., and Whisnant K., " Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.

44 Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, FEBRUARY 2004.

45 APC, Bottom-up Connectivity Strategies: What are the local and global benefits offered by community networks? https://www.apc.org/en/news/bottom-connectivity-strategies-what-are-local-and-global-benefits-offered-community-networks.

5.3 CRs & CNs: Right to co-create internet for equitable internet

Access to information is a backbone of democracy and development enabling citizens to engage in informed decision-making, making government accountable and also socio-economic progress. The right to access information is one of fundamental rights that are defended by civil society organizations and community-led institutions to bring access to information in excluded areas.

The definition of 'digital divide' has shifted its focus from physical access (ICT infrastructure) and affordability (cost of internet connection and devices) to a multifaceted understanding of the causes of the digital divide (UN, 2021)[46], including cultural and social factors, notably the lack of digital literacy and skills and the awareness/relevance of the Internet for disadvantaged people.

Community Radio stations are such community-led entities that are making an effort to bring equitable and uniform access to information in media-dark zone or where accessing information is scarcely available. There are around 4000 community radio stations worldwide (World Association of Community Radio Broadcasters [AMARC][47], n.d). Some of the community radio stations across the globe are given in below table:

India	480+
Bangladesh	18
Nepal	360
Philippines	1000
Thailand	3900
South Africa	290
Australia	450
Ghana	20
Kenya	55+
Uganda	22
So on... in other countries	

46 United Nations (UN), Department of Economic and Social Affairs, 'Leveraging digital technologies for social inclusion'; February 2021.

47 World Association of Community Radio Broadcasters [AMARC] (n.d.). About Amarc. <https://amarc.radio/about-amarc/>.

Most of these community radio (CR) stations serve grassroots communities on broad segments of agriculture, education, health, social security, addressing gender and other local issues. Like CNs, community radio stations are also established and self-managed by communities that built their own infrastructure and technologies to provide the last mile access to the information. CR stations collect, develop, produce and broadcast the content with the help of local people. One of the challenges that CR stations face challenge of having a reliable internet connectivity for broadcasting their programs. While CR stations bring the local knowledge, community engagement and having skilled human resources, community network operators hold technical expertise in setting up towers, resources to manage the local content and services and legal knowledge on radio frequency allocation.

This kind of partnership, as defined by OCED[48] is also an incentive driven since two community-led entities have common goals and interests and money is offered for a certain type of activity or establishing the network. Partnership between community radio and community network also act as cultural actors who manifest themselves as consumers but at the same time as producers who have ability to produce, manage, control the content and host their content and services, efficiently solve local communication challenges and share their culture, while still access accessing, at the same time, the global network under equal conditions as peers. This makes the partnership between the two essential for connecting the unconnected and ability to co-create the internet together.

5.4 CR Bolo: Localised community network preserving local content and culture

India stands as a leader in the mobile internet domain, trailing only behind China in terms of the largest number of internet users globally[49]. This vast user base accesses the internet predominantly via mobile networks, the ITU 2022 shows that 56 per 100 inhabitants have a mobile broadband subscription, versus only 2 per 100

48 OECD, Key Issues For Digital Transformation in the G20; January 2017; <https:// www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>; accessed on 23rd September, 2021.

49 Statista, Countries with the largest digital populations in the world as of January 2023 https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/.

connecting to the internet via a fixed broadband subscription[50]. The COVID crisis has spurred the space of digital transformation, there is an emerging consensus that the digital divide can only be effectively addressed if it is clearly understood, defined and measured through multi-stakeholder approach. In such scenarios, Community networks contributed to provide information services in unconnected regions. However, establishing community networks in rural settings in India without having local organisation support is challenging for any operator.

CR Bolo is such a model that adopts multi-stakeholder approach to provide affordable internet access services in rural Bhadrak district of Orissa. In India, community radio stations in general compliment strengths of community network primarily in five attributes – 1) Infrastructure 2) Technology, 3) Licensing, 4) Local content and 5) Social inclusion and sustainability (Srivastava, 2021[51]). The study identifies that both community-led entities have technologists to maintain and manage the network and also have ability to manage and produce the local content and services and capability to engage with local people.

Understanding that CR stations have great potential to act as a community network operator to provide connectivity services, Jadeite Solutions, a social enterprise partnered with local community radio station – Radio Bulbul to setup the first community radio operated network in Bhadrak district of Orissa. Unlike traditional ISPs, CR Bolo primarily focuses on:

- Engaging with local people and using their capabilities;
- Utilizing and re-using the existing resources and infrastructure;
- Development and sharing of local knowledge and information.

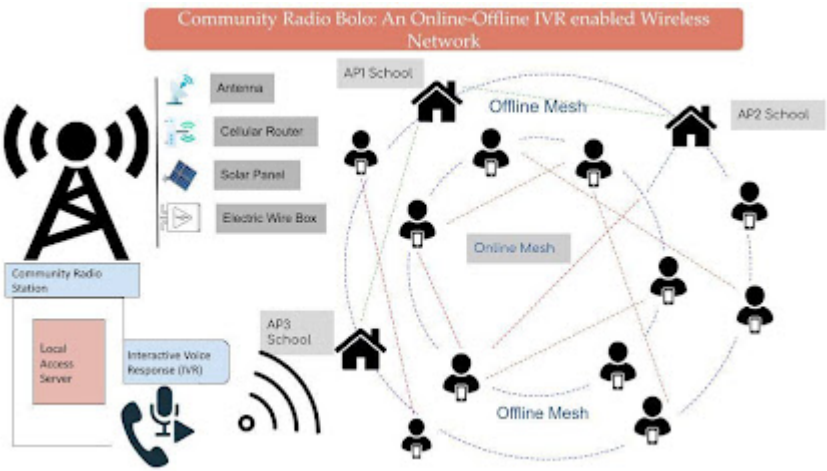
While setting up the community network, CR Bolo, Jadeite Solutions used Radio Bulbul's existing technical infrastructure including radio tower, local server and computers and trained their staff members on managing and operating the network. The CR Bolo connected Radio

50 ITU, Measuring digital development: Facts and Figures 2022, https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/.

51 R. Srivastava, Fostering Global and Local Community Radio Partnerships for Community Network Development: A Case-Study from India, Community Networks: Towards Sustainable Funding Models, Official Outcome of the IGF Dynamic Coalition on Community Connectivity (DC3).

Bulbul with neighbourhood schools and local Self Help Group (SHGs) in radius of 5 to 7 kms through wireless mesh network. CR Bolo uses unlicensed spectrum (delicensed) and other low-cost deregulated media to share content locally, deployed a variety of localized services for sub-communities that curate content for their needs and utilize a hyper-media archive architecture. The local server has been set-up at the station itself for recording, storing local content and feedback received from listeners. In order to provide variety of local channels to communities, CR Bolo coupled the IVR channel to broadcast radio programs along with receiving feedback from communities. The reason for coupling the network with IVR is because majority of the population living nearby Radio Bulbul is school drop-out or semi-literate, hence providing information in local dialect became necessity.

One of the motivation for Radio Bulbul to set up the community network is to develop, share and preserve their local content. Schools used the local network and IVR channel for connecting with other schools and share their content with the radio, whereas women from SHG groups used the services provided by CR Bolo to spread information related to financial services and connecting with other women groups. Through CR Bolo, Radio Bulbul is using variety of communication channels from local network, re-utilizing bandwidth at Radio Bulbul for further distribution in nearby locations. CR Bolo is connecting over 2000 population primarily used by students, SHG women and young population.



To democratize the connectivity, CR Bolo gives flexibility community to use the internet as well as local network to be connected. This way, Radio Bulbul has placed its radio programmes on the local network as well as cloud through which anyone can listen or record the radio programs which have been broadcasted.

Co-designing the wireless network with CR station Radio Bulbul, it helped community radio staff members and local communities to understand their role and responsibilities they hold in managing the network. This also enabled them to understand how to co-create the network by setting up access-points on the basis of community requirements and infrastructure. Community members are not only responsible to manage the hybrid architecture of the CR Bolo network but they are decision makers to identify which access-points should have internet connectivity services.

Following the concept of democratized network, CR Bolo offers the flexibility to locals living nearby Radio Bulbul to use range of communication channels such as local network, IVR, community radio and internet services which allows communities to limit their digital footprint and maintain their privacy without having a fear of missing out information. It helped community to share their experiences and freedom to voicing about their rights and preserving cultural ethics without having a pressure of continuous surveillance.

The physical dimension of the network enables an environment in which locally hosted services and content have no impediments to flourish and be accessible both to the community with or without the internet connectivity and also enable to others outside of the community through IVR channel. This helped the Radio Bulbul to collect local stories from communities, broadcast their radio programs through various channels and also enabling local communities to access and preserve their local culture in a democratizing manner.

As an outcome, CR Bolo is an effort to strengthen community radio stations to understand their potential in providing the last mile access to the meaningful connectivity. These local community-led infrastructure enable communities to preserve to their local dialect, language and culture while accessing the content available on the internet. It is crucial to recognise that such decentralized networks

creates an environment of interconnected that is secure and reliable and make access to communication services as a fundamental right and for human development.

5.5 Why decentralised repository of culture matter?

Globally, there are many community networks and systems that facilitate communication and provide digital services with little or no connectivity, however, when they are fully integrated with the internet, these networks find challenging in adapting? When local community networks compete with traditional providers, their supporting services, creativity and ingenuity made them possible to adapt and sustain. Uniqueness of CNs is distributed and decentralized tools that take advantage of existing intercultural scenarios, enhancing cultural diversity through peer-to-peer communication within and among communities. Because of this, Radio Bulbul is developing the decentralized repository of local content and using local server for storing and distribution of their content.

To design the CR Bolo's repository, the fundamental principle team, followed is to keep the architecture decentralized but organized, so that it is easily accessible by communities. Affordability was another criteria while designing the repository, hence CR Bolo used an open source IVR software that can operate easily on the local network and GSM band and other free tools to deepen the experiences of appropriation of technology in community networks beyond the physical dimension in a real, efficient and valuable way that allows sharing and distributing culture with a counter-hegemonic.

The idea of 'decentralised yet organized' represents two approaches. In the decentralized culture repository, the metadata that makes content organisation possible is replicated along with the content itself. Pieces of the repository that become fragmented still maintain their classification locally. The repository is a natural partner of community networks with little or no connectivity that use sneakernet techniques or narrowcasting to transport information from and to the outside communities that do not have access. Each fragment of the culture repository, which consists simply of a number of instances connected in a network, makes an access point in itself.

This allows for a transparent evolution between the different stages of connectivity of a community network.

Overtime, CR Bolo will become a vehicle to create decentralized network of local access points that create repository of local content and culture, however, when all access points are connected it will create centralized repository of local content and archiving of the culture.

As a local actors, community-led entities need to work in the direction of developing tools or creating affordable and accessible that enable communities in their role as free, sovereign and empowered subjects to produce and share culture. The inclusion of community radio and amateur radios as a community networks in the list can offer some possibilities for grassroots initiatives, especially in rural areas. There is a need of local solutions, which are not top-down business models but having bottom-to-top approach which foster genuine technology autonomy and innovation.

In this way, we need to create flexible frameworks so that the right to co-create the internet can be inhabited by all the people who co-exist in the great global network, creating, in all dimensions, their own internet.

5.6 References

A4AI. (2020). Meaningful Connectivity: A New Target to Raise the Bar for Internet Access. Alliance for Affordable Internet. https://docs.google.com/document/d/1qydsmTY4hln3pP4dWJbCSRFna8SfDYAtGfacKYwhVk8/edit).

APC, Bottom-up Connectivity Strategies: What are the local and global benefits offered by community networks? https://www.apc.org/en/news/bottom-connectivity-strategies-what-are-local-and-global-benefits-offered-community-networks.

Belli L (ed) Community Networks: The Internet by the People, for the People: Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, pp. 153–192.

Best Practices Forum, Gender and Access (2018). https://www.intgovforum.org/multilingual/ content/bpf-gender-and-access-2018.

Bhattacharjee (2021). Community networks: states, solutions and communities; https://genderit. org/feminist-talk/community-networks-states-solutions-and-communities.

Chen S., Iyer R., and Whisnant K. (2002). 'Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors,' In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.

ITU, Measuring digital development: Facts and Figures 2022, https://www.itu.int/hub/ publication/d-ind-ict_mdd-2022/.

ITU. (2023). *Press release*. https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx.

Kim H. (2004). 'Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System,' IEEE Transactions on Consumer Electronics, vol. 50, no. 1, FEBRUARY 2004.

OECD, Key Issues For Digital Transformation in the G20; January 2017; accessed on 23rd September, 2021.

P. Micholia et al., 'Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions,' in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3581- 3606, Fourth quarter 2018, doi: 10.1109/COMST.2018.2817686.

R. Srivastava, Fostering Global and Local Community Radio Partnerships for Community Network Development: A Case-Study from India, Community Networks: Towards Sustainable Funding Models, Official Outcome of the IGF Dynamic Coalition on Community Connectivity (DC3).

Schuler D (1994) Community networks: Building a new participatory medium. Communications of the ACM 37(1): 38–51.

Sloan, P., and Oliver, D (2013). Building Trust in Multi-stakeholder Partnerships: Critical Emotional Incidents and Practices of Engagement. In Organisational Studies 34 (12), p1835-1868.

Srivastava R (2017a) Community networks: regulatory issues and gaps – experiences from India. Available at https://www.internetsociety.org/resources/doc/2017/community-networks-regulatory-issues-gaps-experiences-india.

Srivastava R (2017b) Policy gaps and regulatory issues in the Indian experience on community networks.

Srivastava R (2021); Fostering Global and Local Community Radio Partnerships for Community Network Development: A Case-Study from India; Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity Towards Sustainable Funding Models.

Statista, Countries with the largest digital populations in the world as of January 2023 https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/.

The Economic Times (2019). *How India is using the Internet*. [online] The Economic Times. Available at: https://economictimes.indiatimes.com/%20tech/technology/how-india-is-using-the-internet/articleshow/108354854.cms?utm_%20source=contentofinterest&utm_medium=text&utm_campaign=cppst.

United Nations (UN), Department of Economic and Social Affairs, 'Leveraging digital technologies for social inclusion'; February 2021.

Upasana, Community networks: states, solutions and communities, GenderIT.org, https://genderit.org/feminist-talk/community-networks-states-solutions-and-communities.

USAID and the Digital Impact Alliance (2017) Closing the access gap: Innovation to accelerate universal Internet adoption, https://2017-2020.usaid.gov/sites/default/files/documents/15396/ Closing-the-Access-Gap.pdf.

World Association of Community Radio Broadcasters [AMARC]. About Amarc.

The **authors** of this book are (in alphabetical order): Luca Belli, Sarbani Belur, Felix Freitag, Senka Hadzic, Suruchi Kumari, Osama Manzar, Leandro Navarro, Ritu Srivastava, and Bruna Zanolli.

This book is the Official 2024 Outcome of the Dynamic Coalition on Community Connectivity (**DC3**) of the United Nations Internet Governance Forum (IGF). DC3 is a multistakeholder group, fostering a collaborative analysis of **community networks** (CNs), exploring how such initiatives can improve and expand connectivity while empowering Internet users.

CNs are connectivity initiatives managed according to the governance models established by their community members, in a democratic fashion, and may be operated by groups of self-organised individuals or entities such as non-governmental organisations (NGOs), local businesses or public administrations. This report explores some of the cybersecurity challenges inherent in CNs and what strategies could be implemented to successfully face them. It explores the potential data privacy issues, technological limitations, and the need for incident response capabilities and robust cybersecurity governance. To enhance resilience against cyber threats, the report advocates for a proactive and collaborative approach, highlighting the importance of cybersecurity awareness, training, and investment in security infrastructure. Ultimately, we emphasise that safeguarding the cybersecurity of CN user and assets is crucial for their sustainability and continued growth, ensuring they can continue to provide reliable and secure connectivity.

CNs should not be considered as a competing or antagonistic model either to the state or to the market. On the contrary, they should be seen as a powerful complementary solution to fill the existing connectivity gaps. All previous DC3 publications can be found at **www.comconnectivity.org**.

9 786586 060621