JOURNAL OF PEER PRODUCTION

NEW PERSPECTIVES ON THE IMPLICATIONS OF PEER PRODUCTION FOR SOCIAL CHANGE

HACKTIVISM, INFRASTRUCTURES AND LEGAL FRAMEWORKS IN COMMUNITY NETWORKS: THE ITALIAN CASE OF NINUX.ORG

JoPP Signal:
10/10

Reviewing process: [original] [reviews] [signals]

Community Networks (CN) are an emerging world-wide phenomenon that is receiving growing attention from a number of different disciplines. A CN is an infrastructure for digital communication, an alternative to the mainstream approach of commercial Internet Service Providers (ISPs). It resembles a scaled-down Internet and is used to interconnect a community of people who share particular goals and motivations. By developing a multidisciplinary perspective at the intersection between science and technology studies, law and informatics, this paper analyses the cultural, technical and institutional features of Ninux.org, the most important Italian CN. Ninux.org, based on wireless technology, is made up of more than 320 nodes all over Italy, although mostly concentrated in Rome. This paper provides insights into the political, technical and legal issues of the network, highlighting how tightly interwoven these are, to the extent that they cannot be properly understood in isolation. The paper starts by describing the phenomenon of the CNs; sketching its historical development, the motivations underlying the foundation and use of these networks, their functioning and main legal implications. This introduction is followed by an examination of the specific case of Ninux.org, looking at practices, discourses, and interactions among activists participating in the project. On the basis of this analysis, the paper moves on to consider some technical characteristics and specifications of the network, revealing how the technological infrastructure only partially realises an effective decentralisation and horizontal organisation of the network. We also consider some of the legal constraints imposed by the Italian and European normative frameworks, and the need for Ninux.org to address regulatory issues in the near future. Finally, on the basis of our multi-perspective analysis of this Italian CN, the paper outlines some ways in which the community network could be strengthened, and its participants helped to develop reflexive tools to implement their initial vision of decentralisation.

Keywords:
Wireless community networks, decentralization, Italy, hacktivism, distributed infrastructures

By ***Stefano Crabu, Federica Giovanella, Leonardo Maccari, and Paolo Magaudda***

INTRODUCTION

The Internet is rushing towards centralisation. A small number of network operators, cloud, email and social network services currently handle most of the data exchanged globally on the Internet, thus allowing regimes (Wilson, 2015) and non-regimes (Clement, 2014) to disconnect citizens and control their behaviour. In reaction, attempts to build alternative Internets are made, in an effort to subtract people's traffic from the "black box" that the Internet has become. Since the "Internet" is a mix of cables, routers, protocols and applications, such alternative models and infrastructures for digital communication may involve any combination of these layers. Some well-known examples are the Tor network, the Bitcoin distributed currency, and the Diaspora distributed social network. It is no coincidence that all these projects exist in the software domain: To programme a new application that can compete with existing platforms is far easier than to deploy a new physical network that would tempt a significant portion of Internet users away from the current Internet. Unfortunately, the rush to centralise services is inextricably linked to the physical architecture of the Internet, which cannot be escaped unless that architecture is subverted, or at least complemented.

In spite of the inherent difficulties, some people are trying to achieve this subversion: They are the subject of this paper. Community networks (CNs for short) are digital communication infrastructures that provide an alternative to commercial ISPs. While CNs can be set up with different technologies, since the 2000s they have been primarily developed with wireless technology, which is simpler to set up and cheaper than wired communications. A wide variety of CNs, from small networks to cooperative ISPs made up of tens of thousands of nodes, are now flourishing in many countries.

These alternative networks are usually built and maintained locally by volunteers and activists who share a critical view of the global politics of the Internet. This over-arching political frame present in the experience of several CNs, and especially in the Italian case, suggests that the construction of an alternative local network can be interpreted as a subversive political practice to promote an alternative cultural and political agenda centred on free speech and freedom of information on the Internet. In this sense, a CN is not only a technical infrastructure, but an interconnected "community"

of people, who share the goal of building a fair, sustainable and democratic communication infrastructure. The creation of such an infrastructure is, however, a very complex task, and original conceptions may struggle—and often/sometimes fail—to find concrete realisation.

This paper investigates the experience of an Italian CN called Ninux.org, exploring the discourses and politics developed within the community around the project and analysing how these cultural and social dimensions are effectively translated into the technical construction and topology of the network. Moreover, we consider how CN's political and technical practices can be aligned to national legal frameworks of digital communications. Thus, our analysis will reveal some of the main political, technical and legal implications of the Italian CN, highlighting how closely intertwined these different aspects are, to the extent that they cannot actually be understood in isolation. Inspired by Science and Technology Studies (Latour, 2004) and their aim at disentangling the articulation between the technical, the discursive and the social dimensions of socio-technical phenomena, the paper is intended to reveal arrangements and misalignments that characterise the Ninux.org network infrastructure. Methodologically, the article summarises the results of a research project carried out by a multidisciplinary team of scholars from the social sciences, computer engineering and law. The heterogeneity of the fields involved is reflected directly in the distinct perspectives that emerge from the analysis, in the multiple research methodologies adopted and also in the resultant variety of data presented and discussed. These data include qualitative interviews with participants in the network, a topological analysis of the infrastructure flows, data on participation in the collective mailing list and an analysis of the Italian laws on bottom-up communication infrastructures.

The article starts with an introduction to the technical features of a wireless CN or "mesh network", highlighting the specific properties that distinguish them from home Wi-Fi or larger networks. We present a quick historical outline of these networks, and a review of the recent literature on the social and legal concerns related to them. Then, we move to the case of an Italian wireless CN called Ninux.org, tracing its development from 2001 to its recent expansion. After a description of the evolution of the network, the article presents a detailed analysis of three specific levels of the Italian CN, reflecting the three distinctive analytical perspectives adopted in the research.

The first level is that of the politics and discourses that support and frame the activity of volunteers and participants and their involvement in the construction of the network infrastructure. The sharing of a coherent, but constantly evolving, set of political views about the increasing centralisation of the Internet is a vital driver of participation and is crucial to successful collective negotiations around the shape of the whole infrastructure. The article then moves on to focus on how these political views translate into the material and technical infrastructure topology. Here, we observe that the value of "decentralisation", a crucial element of the participants' political views, is only marginally reflected in the actual shape of the infrastructure, especially when we look at the unbalanced distribution of key roles. Finally, the third level regards the Italian CN's position within the national and European normative frameworks; we consider three of the main legal liabilities, whose unbalanced distribution among users could also contribute to weakening the infrastructure. These three distinct levels of analysis lead us to our conclusion, which highlights the interdependence of the technical, social and legal properties of the network and also offers some suggestions for the future sustainability of the network.

THE TECHNO-SCIENTIFIC BACKGROUND: FROM HOME WI-FI TO MESH NETWORKS

Nowadays, the most common Wi-Fi network architecture is composed of an access point (AP) connected to an ADSL plug: All client devices send their traffic to the AP, which routes the bytes towards the Internet. When two wireless devices want to exchange data from one to another (for instance, a computer communicating with a printer) they still communicate through the AP, even if they are close enough to communicate directly. A CN, in contrast, is, in technical jargon, a wireless mesh network or simply a mesh network (Akyildiz, 2005). In a mesh network, the wireless technology is still Wi-Fi, but there is no AP: when two nodes are in direct communication range they exchange data via the wireless channel, which means that all the nodes of the network are peer nodes.

Communication between two nodes can also take place via intermediate nodes. When Node A intends to communicate with Node B, even if the two nodes are not close enough to communicate directly, the information can be routed via an intermediate Node C, which behaves exactly like the routers that constitute the Internet. Figure 1 represents this situation in a schematic mesh network mounted on rooftops.

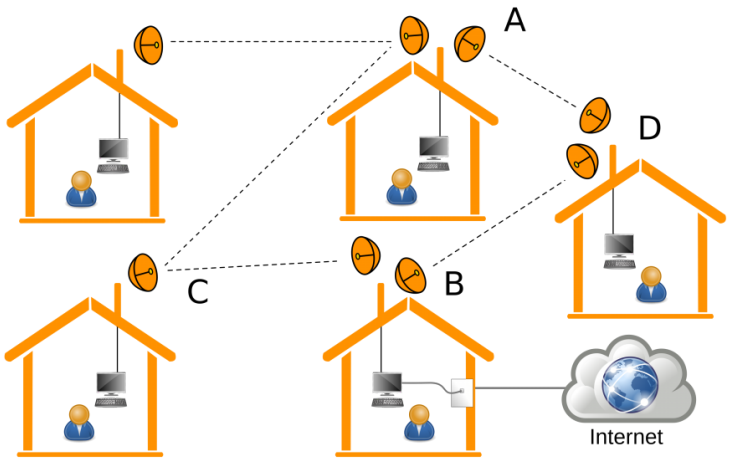

Figure 1. An example of a mesh network with antennas placed on rooftops

A CN is a mesh network in which people install low cost wireless equipment on roofs or terraces, in order to create wireless links with other people. CNs generally develop in an unplanned, organic way. To join the network a new node just needs a line-of-sight connection (free of any obstacle) with at least one of the nodes in the network (modern low-cost devices cover distances up to 20-25km, allowing the creation of city-wide networks). The new node can then act as an entry point for subsequent nodes. Network protocols are designed to enable nodes to be added to or removed without reconfiguring those already running. If we remove Node C, which is lying on the path between Nodes A and B, the network protocols will respond by redirecting the traffic from A to B through Node D, or any other existing path (not shown in the figure). This makes mesh networks resilient to failure: The more nodes in the network, the less important any one node is.

In Figure 1, one of the nodes of the CN is connected to the Internet. For this to happen, at least one user must share Internet connection with the rest of the network, functioning as a gateway. Other users reach the gateway via the CN and from there they access the Internet. In some CNs, either there is no Internet connection, or existent connections rely on individual initiative; in others, associations or real ISPs play the role of the Internet gateway. Mesh networks have been widely studied as a last-mile replacement for Internet access (Baig et al., 2015; Frangoudis, 2011), but a CN is, to all extents and purposes, a small Internet in itself. Participants can install their own servers and host services accessible to all the other members of that network community: These services can include telephony, chat services, file exchange, social networking. The only limiting factors are the personal initiative of the individual user and the available software.

A MULTIPERSPECTIVE OVERVIEW OF THE DEVELOPMENT OF CNS

Even before the mass diffusion of wireless devices, projects focused on the creation of alternative local networks had proliferated. Since the initial development of the Internet, alternative local networks have been sustained by countercultural views on information technologies and by the idea that the Internet should be a liberating tool in the hands of the people, not a means of government control. Historically, the first example of a CN could be considered the “Memory Project”, established in Berkeley in 1973; its functions and services embodied the countercultural and democratic instances, widespread in that period among the youth (Levy, 1984). In the 1990s, CNs created and run by users grew in significance, carrying a distinctive set of political and cultural assumptions about the role of local communities and users in the development of digital networks: The Seattle Community Network Project, for example (Schuler, 1994). In this same period, in the U.S. especially, a generation of community networks was developed to support local development; they, for example, offered commercial and administrative services, in tourism, emergency management and other fields (Carroll and Rosson, 2003, 2008). However, as Tapia and Ortiz point out (2010), projects supporting these local networks created at the municipal level were frequently characterised by a “deterministic” approach and often did not produce their expected outcomes in terms of participation and democracy. In the 2000s, the diffusion of low-budget wireless technology enabled CNs to emphasise the importance of establishing an autonomous hardware infrastructure, allowing the creation of small independent networks in both Europe and the U.S. (De Filippi and Tréguer, 2015).

The particular significance of CNs arises from the fact that these networks are created by groups of people who develop a common project and share distinctive views about the meanings and values of their work (Shaffer, 2011; Söderberg, 2011). CNs rely on working groups, who share some degree of identification and involvement in the project (Antoniadis et al., 2008). In several cases, public or local institutions support CNs, seeing them as experiments in civic participation, or bottom-up solutions for digital divide issues (Powell and Shade, 2006; Carroll and Rosson, 2008). For all these reasons, knowledge of the social and cultural backgrounds of the groups and individuals participating in a CN is necessary to their understanding: Approached from a purely technical and organisational perspective, a CN can only be understood superficially.

In the last 15 years, a basic set of political motivations has emerged from the intersection between CNs and new media hacktivism (Lievrouw, 2011). Community networks represent the latest incarnation of a long historical tradition of oppositional and radical media, such as pirate radio in the 1970s (Atton, 2002; Downing, 2000): motivations for building CNs are directly linked to emerging political practices grounded in critical views about informatics, software and the use of the Internet. Particularly after the Edward Snowden scandal in 2013 and the recent mainstream visibility of Anonymous cyber-political actions, public concern about Internet privacy and control has greatly increased, thus turning CNs—especially wireless ones—into a strategic topic for countercultural and social movements (Milan, 2013; De Filippi and Tréguer, 2015). As Söderberg has argued (2010, 2011) considering the Czech wireless network community, the sharing of a political conviction is a key driver of participation in CN projects. Soderberg also showed that although political ideas are fundamental to the projects, they are not static, taken-for-granted frames; in fact, it is important to realise that the political beliefs of participants in CNs are constantly negotiated and redefined, as, for example, when market opportunities became a possible option.

A key technical feature that frames political discourse in the CNs is their *distributed* and *highly decentralised* nature. In distributed networks, users cannot be easily “disconnected” and as long as there is a path from source to destination, communication can take place. Referring again to Figure 1, the nodes that have more than one link will be connected even if some of their links fail; at a network scale this means that no single point of failure has been intentionally introduced, and therefore there is no “kill switch” that can be used to shut down the whole network. For the same reason, there is no central point through which all the data are forced to pass, which makes the network harder to spy on, to filter or to control in any way. A decentralised network also enables decentralised ownership, in many cases no single entity owns the network, and no one person can be ordered to switch down or censor the network. These features potentially apply to any distributed network and they are central to the sense of independence and autonomy shared by CN activists. However, in fact, not all distributed networks operate in this manner. In the paper, we will discuss to what extent such properties are actually embodied in the material architecture and maintenance of the Ninux.org infrastructure.

While political motivations have inspired many of these projects, a crucial problem for the development of all CNs is the scaling up of the number of activists, and reaching an audience larger than the initial group of computer geeks. The size of the network is not only a metric for its success: as we have said, the more nodes a network has, the more resilient is its structure. Moreover, size is also a driver for growth: The larger the network, the more likely it is that people are close enough to an existing node to be able join the CN—the phenomenon resembles in some the economic concept of the “network effect” (Liebowitz and Margolis, 1994; Page and Lopatka, 2000). A key growth factor for a CN is the choice to provide Internet

access. Networks that provide Internet access in competition with commercial ISPs usually attract a larger number of people than those that just focus on local services. On the other hand, local services leverage on the various technological features that distinguish the communication inside a CN from a standard Internet connection, primarily the fact that the capacity of the links can be very high; using affordable outdoor devices one can set up wireless links that offer a throughput of up to hundreds of megabits per second, way more than the typical ADSL. Delays are also smaller than with ADSL connections, this is particularly important when using real-time services, such as voice or video transmission. Secondly, commercial ISPs assume that users are more interested in downloading than uploading contents, and ADSL lines are therefore asymmetric—it is faster to "download" than to "upload" content. This means that networks that focus on local services, rather than Internet connectivity, are the perfect playground in which to develop peer-to-peer applications, and attract a smaller but more motivated and tech-savvy participants. These two different evolutionary trajectories (leading either to a cooperative ISP or to a local-only network) are not necessarily mutually exclusive, but they compete to access the limited time and resources available to people involved in a CN.

Finally, it is important to emphasise that the architecture of CNs is also conditioned by the legal framework in which they develop: Regulation can be either a tool to support and reinforce CNs, or a hurdle that hinders their growth. From a legal point of view, CNs represent a new instance of an old problem: When dealing with a new technology, law needs to evolve and adapt (Pascuzzi, 2010). The main difficulty in analysing CNs from a legal perspective is their technical and organisational architecture, which makes it almost impossible to apply classical legal tools, such as civil liability, to them (Dulong de Rosnay, 2015; Giovanella, 2015). Indeed, while some CNs are part of bigger projects like foundations or associations, others are the result of completely spontaneous movements (De Filippi and Tréguer, 2015: 3-4). In the latter case, the bottom-up approach of a CN is often reflected in the absence of a hierarchical structure and, most importantly, in the lack of a central controlling administrative body, or even one with representative powers. This implies a lack of "legal personality", which means that it is impossible to ascribe liability to the network as such (Giovanella, 2015: 59 ff.). Parallel to these peculiarities of the network's structure, the internal functioning of the community also entails legal implications. For instance, the high level of anonymity, enhanced by the fact that there is no database of users' information—even of Internet Protocol addresses—is of great value to CNs, and promises huge potential for freedom of speech. However, it also makes it very difficult to enforce rights violated either within or outside the network (Dulong de Rosnay, 2015: 3-4; Giovanella, 2015: 54 ff.).

CNs are thus revealed to be a complex and multidimensional phenomenon, which can only be fully understood if examined from a number of different perspectives. In the next section, we start describing the Ninux.org project by focusing on its historical trajectory.

BIRTH AND KEY DEVELOPMENTS OF THE ITALIAN CN NINUX.ORG

The Ninux.org project is part of a recent revival in the development of community networks across Europe. Thanks to wireless technology, the last ten years have witnessed the birth of several projects aimed at building grassroots community networks, based on communities of activists and driven by different needs and demands (De Filippi and Tréguer, 2015; Shaffer, 2011). FreiFunk in Germany, AWMN in Greece, and Guifi.net in Spain are among the most important European CNs.[i] The latter, started in Catalonia in 2004, is the biggest of these, with more than 80,000 current users, who are mainly attracted by the Internet access offered, with its independence from any commercial ISP. Other networks, such as FreiFunk in Germany and Wlan Slovenija, did not develop primarily to compete with traditional commercial ISPs; their key driver was political activism around the importance of decentralised networks in a digital society. In these last cases, while they were inspired by political ideals, communities needed to offer convenient services to users in order to scale up from the narrow niche represented by media activists or experts to a larger group of people (De Filippi and Tréguer, 2015: 6).

The Italian wireless community network project started in Rome. From the beginning, it adopted the name of Ninux.org and—especially over the last few years—has expanded rapidly now identifying a national platform which brings together several independent urban-based "islands". The biggest, most important urban network is still that of Rome, where most of the approximately 330 national active "nodes" of the network are located (see Maccari, 2013). The project originated in Rome, where in 2001 a group of students and hackers started experimenting with grassroots wireless networking, following the recent example of Seattle Wireless, created in 2000. As some of the participants interviewed for this research reported, a turning-point in participation took place around 2008, primarily as a consequence of the lowering of the costs of wireless equipment (antennas and especially routers), which led to an increase in the numbers of individual antennas installed on the roofs of participants and their friends. The "island" of Rome served as an example for the development of local wireless networks in other Italian cities, such as Florence, Bologna, Pisa in the north and Cosenza in the south. While the infrastructure in Rome now includes a significant number of "nodes" and has become a reliable network for hundreds of people, the other "islands" are still at an experimental stage and their networks do not yet extend beyond a core group of experts and activists.

Although the general technical and political framework of the local "islands" is the same, their connectivity and organisation has developed independently, and their respective working groups are driven by distinctive mixes of political, technical and local needs and motivations. For example, while Ninux is still informal and non-institutionalised, other "islands" have established various kinds of indirect relationship with institutional actors, ISPs or universities. The primary motivation behind some of the "islands" is the political desire to challenge the perceived neoliberal governance of the Internet; other "islands" are also driven by strong political ideologies/beliefs, but are not a priori against the inclusion of market processes within the building of their networks. Therefore, although they arise from similar backgrounds and political ideas, each CN is characterised by a slightly different combination of cultural backgrounds and degrees of political mobilisation. In the "island" of Pisa, participants are closely interconnected with student leftist associations and the squatted, self-managed social centres, known as *centri sociali autogestiti* [CSA]. In Florence, key participants in the network came from previous experiences of media activism, including involvement in the open software movement. The activists of the smaller network in Bologna are a mix of technology enthusiasts, often university students, and activists from a squatted CSA in town.

Although independent of each other, all these networks are part of the wider national project, Ninux.org, which serves as a common working platform for all the participants. The Roman network and the groups in some of the other cities directly involved in the project share a common vision of the role of CNs in society, and of the general direction in which the networks should develop. This common view was negotiated collectively and

can be found in a “Manifesto” available on the project’s website; [ii] each participant in Ninux.org is the owner of their own node, and has to adhere to the Ninux manifesto, which is largely based on the Pico Peering Agreement [iii] applied by several other international CNs.

The manifesto highlights a number of important points which reflect the heterogeneity of the questions covered by the projects, including: the crucial importance of the technical choice to design decentralised and mesh architectures; the role of the CN as a democratising tool and as a resource to bridge the digital divide; its connections with issues around freedom of expression. These examples reflect the whole set of needs, motivations and political drivers that sustain the discourses and practices of the Italian wireless community network.

Finally, we highlight the crucial aspect of the various forms of digital communication adopted by the CN’s activists. The mailing lists used by the different islands that constitute Ninux.org are currently important instruments of coordination and collaboration, in combination with face-to-face meetings. The usual procedure is that each island arranges its own mailing list, to which any member may sign up, thus gaining the right to participate in ongoing discussions. The mailing lists are a communication device for sharing the minutes of meetings, proposing technical solutions for current problems, alerting on new technical problems in need of fixing, and giving information regarding national and international events which may be of interest to the community. These contents are vital to the management of the community and Ninux.org’s members therefore archive (in a website accessible to anyone, at any time) all the communications made on their mailing lists, thereby shaping a digital collective memory related to the construction processes of the CN.

POLITICS AND DISCOURSES IN THE NINUX.ORG COMMUNITY

In this section, we concentrate on the ways in which the Italian community network embodies specific political visions and motivations, and how these cognitive and discursive elements intersect with the technical and material evolution of the network. These reflections are based in an STS (Science and Technologies Studies) perspective, which allows us to study the constitutive entanglement of the social, the political and the technological in different situated settings of interaction (see Callon et al., 2009; Brown, 2014). This theoretical tradition helps to highlight how closely connected—entwined, in fact—the technical dimensions of CNs are with the political and cultural frames shared by activists. It also enables us to reveal the tensions and negotiations between technological elements and political claims connected to a critique of the evolution of Internet governance, and of networking technologies in general (McCaughey and Ayers, 2004).

An initial point is that, while Ninux.org is an informal organisation without strong ties to specific political traditions, many symbolic and discursive elements shared by CN activists are part of a broader Italian antagonist movement focused on ICT (Pasquinelli, 2002; Beritelli, 2012). These political ideas connected to media and technology have gained particular relevance since the anti-G8 protest in 2001, which helped to strengthen the media-activist movement, and encouraged the spread of informatics-based protest activities within the numerous squatted social centres across the country.

Genealogically, the Ninux.org community is a socio-technical setting for a range of experimental and innovative ICT activities. Our analysis of the different logics of participation in the project begins with the words of one of its most active members:

> These networks are the culmination of all geek knowledge. Within the framework of these projects, if you’re a geek, you can find everything you love: from the development of software, up to building an antenna with a soldering iron […] and whatever. [Public presentation of the project, Bologna, 28 March 2014]

This quotation draws attention to the fact that a CN is a collaborative space within which members share their passion for a set of activities related to the manipulation of devices and technological equipment which, ultimately, allows the building of a wireless infrastructure. From an organisational standpoint, the CN brings together a group of people who want to design a specific techno-scientific innovation project, in which the boundaries between the roles of the user-activist and innovator-experimenter—involved in handling heterogeneous technologies, in installing an antenna, or in creating new software—are merging and imploding (Oudshoorn and Pinch, 2003).

Participation in the Italian CN is rooted “in” and juxtaposed “with” cultural frameworks, densely connected by political aspirations and claims concerning the critical use, and appropriation of, ICT. In this context, political ideas should be seen as drivers of practices intended to construct an alternative digital communication infrastructure and thus escape the current global governance of digital communication, which is increasingly shaped by the “neo-liberal paradigm” (Chenou, 2014; Pelizzoni and Ylonen, 2012). The predominant political stance of the Ninux.org community is its critique of the contemporary global organisation and governance of the Internet, which can be understood as a result of the juxtaposition of technological, scientific and legal devices. This complex assembly of techno-scientific and normative elements circumscribes the regulatory architecture of the relationships between social actors and the Internet infrastructure, shaping its proprietary borders, contents, modalities of access to services, and participation. Indeed, critiques of current Internet governance run consistently through the narratives of members’ participation in the CN:

> Just the fact that someone says: “Sorry, but Internet is not already working? Why is it not enough to request to the municipality to put Internet in areas where there is not?” This statement is a challenge for us, and we want to do our contribution in building a parallel infrastructure, which has grown over time, is growing now, and represents a space of freedom. The central aspect is the possibility of being able to manage your services, to be able to create from scratch the stuff that the community around you needs. And then, the fact that more and more, at the global level, Internet issues remain a central concern in terms of the development of contemporary capitalism. Therefore, it is important to cultivate an experience that is rebuilding from scratch a community: A network that can work, and at the same time forces you to put into question what are the challenges of this great battlefield. [Member of Ninux.org in Pisa].

This quotation reveals a particular political position, which is shared by almost all Ninux activists and is crucial to their collective action and participation: The Internet is not considered a neutral tool for digital communication, but rather an infrastructure permeated by specific negative

functional logics that should be challenged. These negative aspects include the centralisation of infrastructure ownership, the subordination of citizens' privacy to data control, and the general predominance of commercial and profit-based Web services over non-profit and more democratic and horizontal platforms. Therefore, the crucial political question raised by community networks like Ninux.org cannot be confined to the technological dimension alone. Indeed, CN projects demonstrate that shaping an infrastructure from below can become a strategic action to cope with the neo-liberal governance of the Internet. In this sense, a spontaneously built distributed infrastructure, with a bottom-up approach, represents a translation of political visions into a material network aimed at cultivating and sustaining practices of cyber-resistance. In so doing, activists define innovative concepts of the relationship between citizens and communication technologies, and provide alternatives to the hegemony of the neoliberal paradigm.

However, while political motivations are widely shared and are the basis of a common identity within the project, there is no cohesive view on the way these political stances can be married to technical choices and targets. This is particularly evident when the smaller and more politicised local "islands", like Florence and Pisa, are compared to the trajectory of the larger Ninux local community in Rome.

During our empirical research, these political motivations were particularly emphasised by several activists in the cities where Ninux.org is still taking shape, like Pisa, Bologna and Florence. On the other side, the gradual extension of the network in Rome has generated tensions with regard to the extent to which political ideals and goals should be prioritised and this may undermine technological experimentation, in the interests of infrastructure management and maintenance. More precisely, the tension between technological experimentation and the need to ensure stability for a large distributed infrastructure arises from the presence of different visions of how the community network should be realised. Consider the following thoughts from a veteran activist of Ninux.org in Rome:

> Long time ago, people who started to participate to Ninux.org had strong skills. Instead, now people know the project through advertising on Facebook. I know this has meant that the community has become so large, and the network is extended. But, obviously, the average technical expertise has dropped far. And then, when you propose to change something, it is very complicated to make it acceptable, because many members do not understand it. They do not know how to handle it. Members are convinced that what we have now is already enough. So, they do not feel motivated to change, or to walk through new ways. [Member of Ninux.org in Rome]

This reflection demonstrates how relationships between activists, their political aspirations, and technologies can shape a conflictual socio-technical space. This terrain may be connoted by tensions and negotiations pertaining to the boundaries between the implementation of consolidated knowledge and technological solutions (which already work), and the push to experiment and develop new skills and knowledge which can translate political ideals into an alternative network that embodies innovative concepts of ICT use. From this perspective, Ninux.org appears not as a fully coherent and cohesive technical and political project, but rather as the result of a plurality of visions, as when, for example, the need for network technical reliability and efficiency hinders continuous experimentation.

This section has highlighted how political ideas and practices are a crucial element in the fostering of the CN's construction and maintenance. At the same time, we have seen that the participants' visions do not form a monolith, but rather a complex set of shared beliefs constantly negotiated around political demands and technical work.

ENTERING THE NINUX.ORG DISTRIBUTED TECHNICAL INFRASTRUCTURE

We have discussed how the origin of Ninux and the motivations for its development are deeply rooted in a critique of the current organisation of the Internet, its governance, and the predominance of a service model in which the user gives away all control of the instrument he/she uses. Ninux tries to build an alternative model in which the network has no owners, no single point of failure (or control), and the community itself tries to avoid hierarchical social organisation. This section describes our analysis of the extent to which the spirit that initially animated the community is effectively translated into the realisation of the network, and how present it is in community interactions.

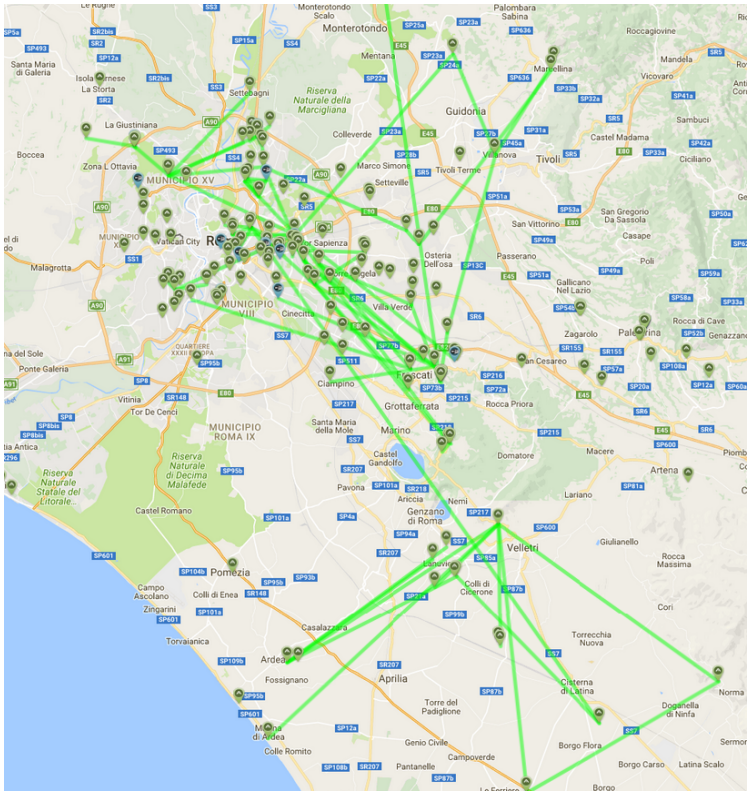

Figure 2. Topology of Ninux.org in Rome

Figure 2 gives a snapshot of the current topology of Ninux in Rome, taken from the mapserver on the Ninux.org website. The *mapserver* [iv] is a key asset of the Ninux community, and of many other communities: When a new member wants to join, he/she enters his position in the *mapserver* and creates a "potential" node, and is then a placeholder expressing an interest in joining the community. He/she can then be contacted by other people with nearby nodes, through whom he/she joins the network. A node passes from a "potential" to a "running" state when it has been physically installed and connected to the rest of the network: At that moment, it becomes part of the network.

While conducting our research, we had access to the Ninux database, with all its nodes and their owners and links. We extracted the full network topology of Ninux and represented it as a graph: A set of nodes (that represent the wireless routers) connected by a set of edges (that represent the wireless links). We only analysed the largest component of the graph—the Rome Island—and, after aggregating the nodes placed in the same location, extracted a graph made up of 140 nodes and 158 edges. We omit many details of the data collection that can be found, together with the source code and the data-set, in previous studies (Maccari et al., 2015).

Our goal was to perform a technical analysis of the network graph to outline some criticalities and correlate them with the data on the structure of, and participation in, the network. We therefore computed three metrics on the graph to complement the qualitative analysis described above, and to help us understand the extent to which the network can actually be considered "distributed". These three indices are: group betweenness, the ownership distribution of nodes and "owner betweenness". The group betweenness approximates how much traffic passes through a group of nodes, and can be applied to any graph, like a communication network or road map. More precisely, to compute the betweenness of a node *k* one has to consider all the possible pairs of nodes *(i,j)* in the graph, and compute the shortest path between each couple. The shortest path is the shortest sequence of nodes in the graph that must be traversed to go from *i* to *j* and, in the network graph, it represents the path that data follows when node *i* communicates with node *j*. The betweenness of node k is the number of shortest paths that include *k*, normalised by the total number of couples in the graph. This concept can be enlarged to a set of nodes: The group betweenness of a set of nodes *K* is the relative number of shortest paths that pass across at least one node in the group *K*. In practice, given a set of nodes, the group-betweenness expresses the total portion of traffic that these nodes may be able to intercept. We can also reverse the point of view. Let us suppose that an attacker wants to intercept as much traffic on the network as he/she can, but to do this he/she is only able to attack and control a limited number of nodes: Group *K*, with the highest group betweenness, is the best target to choose. We computed the group with the highest betweenness for groups of size 1 to 5, reported in Figure 3.

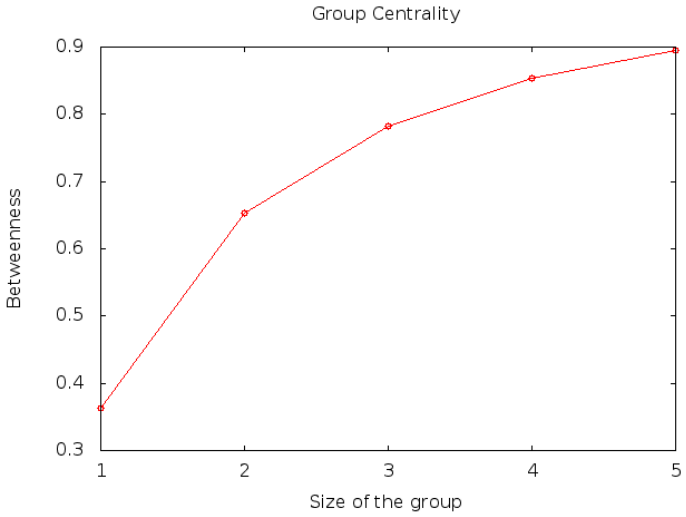

Figure 3. Group centrality in the Ninux network

Figure 3 shows that an attacker who could choose no more than 5 of the 140 Ninux nodes, would actually be able to access almost 90% of the total traffic generated. We have also observed this behaviour in larger CNs (Maccari et al., 2015); it shows that the fact that a network is "distributed" by no means guarantees that it has no critical nodes. Indeed, the control of a very small fraction of nodes would allow someone to spy on most of the network's traffic, probably because of how the network was designed/built. Usually, a CN starts with a few small disconnected islands inside a city; these islands then become connected to each other when a new node is placed in a dominant position (a hill, a tall building etc.). This new node suddenly starts routing a large portion of the traffic, leading the community to start investing in its infrastructure, by adding new radios, for instance. This of course makes it even easier to connect to the node, and creates a vicious circle in which the community invests heavily in a few important nodes, thus unconsciously re-creating a hierarchy among the network nodes.

Something similar happens with the ownership of the nodes. Figure 4 reports the distribution of the nodes owned by each individual. In the node database, a contact email is associated to each node; we aggregated the nodes corresponding to similar emails using standard comparison procedures (Bird, 2006) and human checking. Although there is room for potential error, the trend described is clear. [v]

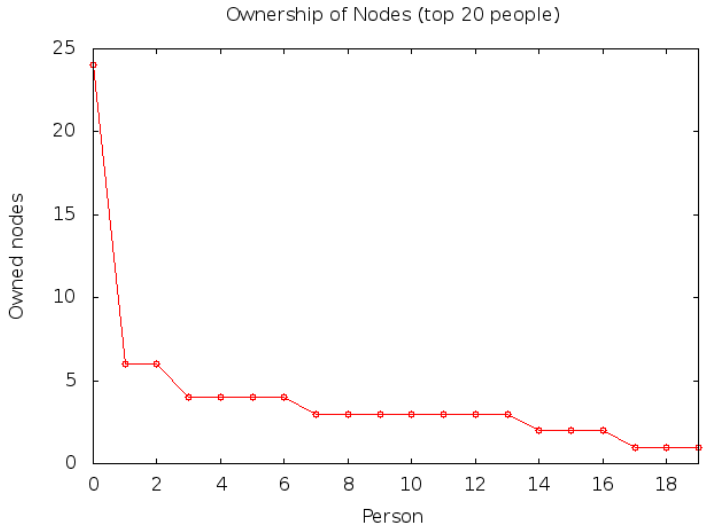

Figure 4. Number of owned nodes per person (top 20 people)

The distribution in Figure 4 is skewed, among the 78 people who own at least one node, 61 own just one node, and 17 own more than one. The top person owns 24 nodes, the top 5 people own 44 nodes and the top 13 people own half of the nodes in the network. The explanation is easy: there are a few people—one in particular—who are highly technically skilled and help many newcomers to set up their own nodes. So, even when the nodes are not placed in a location physically owned by the same person, that person is nonetheless the one who installs and manages them.

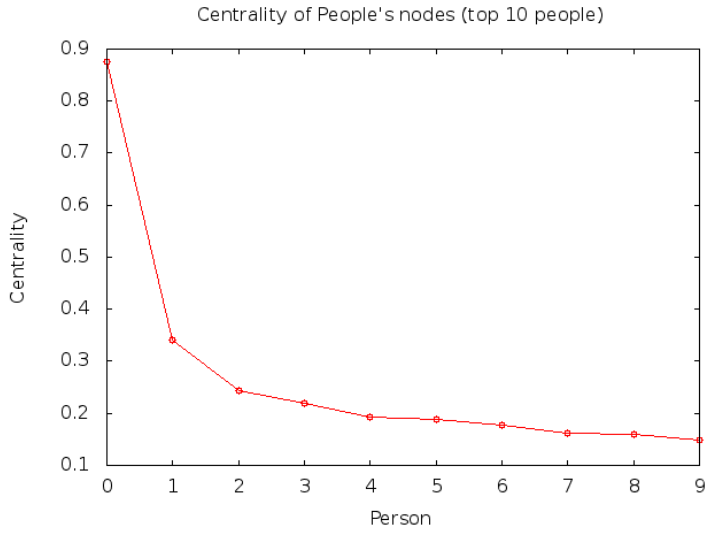

Figure 5. The person centrality in the Ninux network

The two graphs already shown are combined in Figure 5 to show the "person-centrality", that is, the amount of traffic that could be intercepted by a single person through the nodes he/she owns. Unsurprisingly, the graph shows that there is a small group of people (and one in particular—the top owner of nodes) who could easily intercept a non-negligible amount of traffic. Again, the spontaneous actions of the most skilled and collaborative people in the community create a single point of failure for the network.

Finally, we present a preliminary analysis of the mailing list of the Rome Ninux Island. The data refer to approximately one year of discussion and show the normalised number of answered emails per person. This is a very basic metric to determine how influential someone is in a mailing list; the rationale behind it is that the more answers someone receives to an email, the more interest they can raise in their topics.

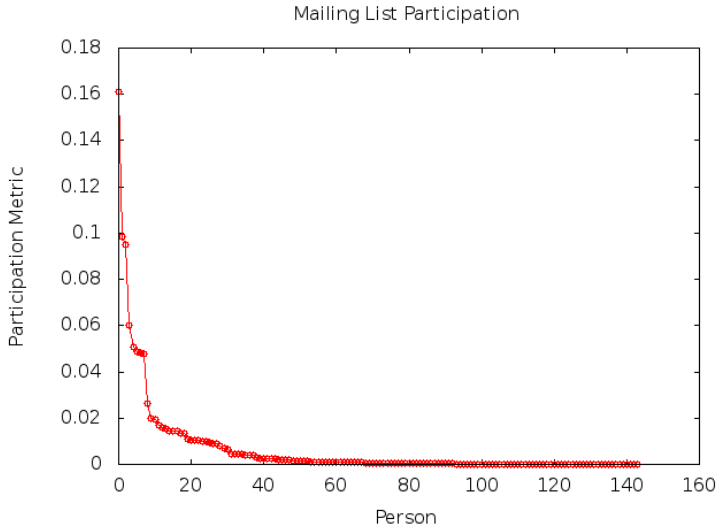

Figure 6. The participation metric in the Ninux mailing list

Figure 6 shows that the mailing list seems to be dominated by a few individuals, who monopolise its discussions. We wanted to ascertain whether there was a correlation between the ownership of nodes and mailing list activity; this correlation does indeed exist. For each person, we have introduced a combined metric which takes both quantities into account. [vi]

The following graph was obtained:

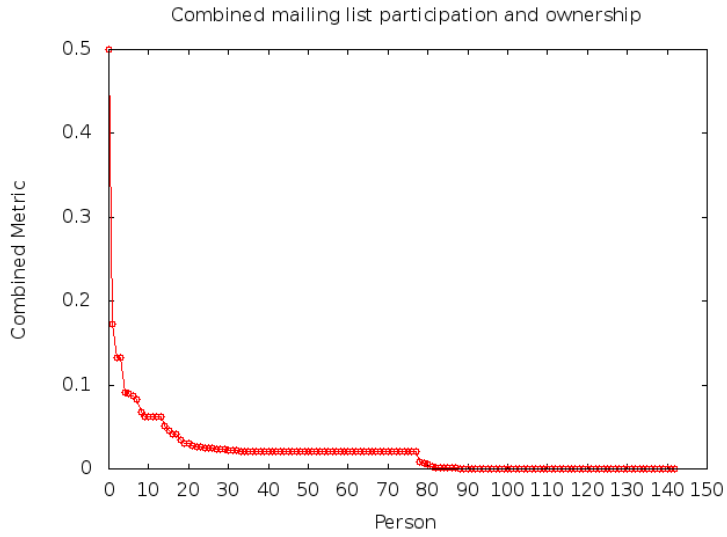

Figure 7. Combined relevance metric in the Ninux network and mailing list

This graph, too, is very skewed towards the high values, effectively showing that only a small fraction of the people who write in the mailing list or own at least one node actively participate: The majority merely contribute to the community marginally.

The data we have analysed so far show that, despite the community's intention to create a decentralised, community-managed network that offers some protection against intrusion, the actual implementation diverges from the original intentions. The network is pretty concentrated (as few as five nodes could in principle intercept 90% of the traffic), the ownership of the nodes has a skewed distribution, and participation in the discussion mailing list is, again, largely limited to a few individuals. The reasons for this again lie in the spontaneous development of the network, in which only a few people are really active, leading the discussion and practical development of the network. This is not peculiar to Ninux; the same topological features have also been found in two other community networks (Maccari et al. 2015), since it is a product of the spontaneous growth of the network. In other words, the fact that a network is unplanned does not necessarily facilitate the development of a genuinely decentralised architecture.

This quantitative trend towards the hierarchisation of the mailing list discussion is the gradual outcome of a wider process driven by factors such as degree of motivation to devote time to the project and other heterogeneous capabilities—like technical and coordination skills—through which Ninux.org's members develop and elaborate their reputation, membership, roles and authority within the community. The highly centralised participation in the mailing list also emerges from a reading of the content of the discussions that take place in this digital communication space. The most active members in the mailing list seem to be a niche of activists to whom the task of introducing and coordinating the key, decisive discussions about infrastructure management, maintenance, and development strategies has been informally "delegated". From an analytical point of view, the technical skills required to sustain this discussion and manage the network are not horizontally distributed, thus leading to the polarisation of "decision making" about the management of the community. The fact that a small core group of activists does almost all the coordination of the technical maintenance and management of the infrastructure is also reflected in the vertical participation in the mailing list discussions, within which the discourse and the management framework that support the CN are defined.

Counterintuitive as it may seem, a certain amount of coordination and monitoring is necessary to maintain a high level of distribution within a decentralised network and its community, as we suggest in our conclusion.

NINUX WITHIN THE ITALIAN LEGAL FRAMEWORK

The legality of a new technology is key to predicting if and how it will evolve and prosper. This section therefore explores some of the legal implications of the political and technical features of Ninux.org. By analysing the legal context within which the CN operates, we want to shed some light on the very real possibility that Ninux.org could be the target of legal actions, which might represent a point of failure for the network.

The current Italian framework for electronic communications (Electronic Communications Code: d.lgs. 1.8.2003, n. 259, as amended), which largely derives from EU law, allows the creation and diffusion of Wireless Community Networks (such as Ninux.org) without the need for any authorisation. In fact, the technologies on which CNs rely are considered to be free activities (Giovanella, 2014: 960 ff.) and the creation of a CN can be considered legal, as it is not explicitly prohibited. While previous Italian legislation would have impeded the flourishing of these communities, the current framework does not.

On the question of civil liability, and taking into account the different subjects involved in a CN, three liability situations in particular can be imagined (Giovanella, 2015). First, a user could personally commit an illicit action within the network, and would consequently be liable for his/her own conduct on the basis of the general rules of civil liability (i.e., for the Italian context, Art. 2043 of the Civil Code). The first step in the enforcement of a violated right would be to identify the alleged infringer. This, however, may be very hard to do, depending on the way in which the CN in question is managed. In Ninux, there are no designated identification numbers: Each user has an IP address but chooses her own number, which may then be changed at any time. Moreover, these numbers are not registered on any database, even though the Ninux website includes a table displaying the IP numbers chosen by the users. Although this rough database seems to provide important information for tracing IPs back to real identities, [vii] the table is actually easily modifiable and falsifiable and cannot be considered a reliable tool for this purpose, so that the possibility of identifying the

wrongdoer is dramatically hampered. The same problem arises if a user is routing someone else's illicit data; even in this instance no user can be identified and held liable.

A second possibility is that an illicit action may start within a network but be directed outside it through a gateway. Each gateway node in a CN can be identified by its public IP address; the gateway's provider could then match the access data with the identification data of its customer, thus obtaining the real identity of the gateway owner. In such a situation, the ISP supplying the Internet connection to the gateway user may be brought in as a defendant and the European Directive 2000/31/EC on "Electronic commerce" and its implementation would then apply in all EU Member States. [viii] This Directive regulates the liability of providers for third party civil wrongdoings. Under it, if an ISP complies with the specific conducts prescribed by the law, it will not be held liable for a third party's conduct (Baistrocchi, 2003; Verbiest et al., 2007). The Directive divides ISP activities into three different categories: mere conduit, caching, and hosting (Arts. 12-14). In Italy, the implementation of the Directive was made verbatim with d.lgs. 30.4.2003, n. 70 (specifically, Arts. 14-16). Under Art. 12 of the Directive (Art. 14, d.lgs. 70/2003), ISPs that only offer a connection to the Web are to be considered "mere-conduit" providers; they are probably the most relevant to our current analysis. There is a binding contract between the ISP providing connection and its customer: A provider can limit its own responsibility by means of specific contractual provisions that expressly forbid the customer to share the connection. Contractual provisions of this kind already exist in various contracts. [ix] In such cases, the customer/node-owner that opens her node to her peers would thereby breach the contract. In addition to being liable for breach of contract, the customer could also be considered liable for the damages suffered by the provider as a consequence of the illicit conduct committed through the gateway (Giannone Codiglione, 2013: 107; Mac Síthigh, 2009: 366-369; Robert et al., 2008: 217 ff.). This imposition of liability on the single customer or user could be a deterrent to sharing her connection with unknown or unreliable users. [x] More generally, this might represent a deterrent to opening up the CN to the Internet. This analysis, which is based on Italian legislation and on the case of Ninux, can probably be extended to other European communities, even though each Member State may have implemented Dir. 2000/31 in its system in slightly different ways.

The above discussion can be directly connected to our technical analysis, since if the gateway node is one of the few critical ones upon which the network relies, such a scenario may constitute a danger to the network's stability and robustness. If the most important nodes (i.e., those that carry more traffic and keep the network connected) are also gateway nodes, their owners are the easiest targets for possible legal actions. Since a legal action can greatly discourage people from active involvement, it is advisable to separate gateway nodes (and their owners) from critical nodes in the topology (and their owners). A third possibility is that the CNs themselves could be considered to be accountable entities. More precisely, if the bottom-up approach reflects a total absence of organisational structure, no legal personality exists and the CN cannot be sued. On the other hand, if a CN is organised as an association, specific liability regimes apply (e.g., Arts. 14-42 of the Italian Civil Code). In this event, there would be a legal representative, in the form of a committee or a president of the association, who could be held liable for members' actions. This would also entail certain consequences in terms of being more easily controlled from outside.

Whether a CN chooses to organise itself as an association or not may entail positive and negative effects. Among the former, an obvious example is the possibility of obtaining public and private subsidies. A formalisation of the network might also help in cases where the network wants to function as a kind of lobbyist. A possible negative effect might be that the need to organise the governance of the network and to share the burden of accountability among certain members might make the network structure become too rigid, thereby losing some of its "genuineness". In addition, if we take Ninux as a representative example, based on the empirical analysis illustrated in Section 3, it is plausible that organisational roles will be assumed by the same people upon whom the survival of the network depends. These people are indeed the most interactive, the most involved, and those who care most about the health and continued survival of the network. It would therefore be natural for them to take on organisational and accountable roles if a network-association were to be formed. In some ways this overlap between ownership, control and responsibility might be desirable: As our analysis illustrates, some coordination is necessary if the network is to retain its clearly decentralised structure. If the owners of critical nodes also have organisational roles, the entire network can be more easily coordinated and monitored. On the other hand, this might also threaten the stability and robustness of the network and its sustainability. Let us imagine that the association is sued; one of the people in charge of the association would represent the entire network and could be considered liable for all the infringing activities that had taken place within the network. This could lead to the shutdown of a node, either following a judicial order or because the owner no longer felt like maintaining it. Whatever the reason, if someone owns a critical node, the shutdown of that node could compromise the functioning of the entire CN.

Given all of the above, a CN's choice either to organise itself as an association, or not, and the way in which this choice is put into practice, becomes very significant. We have already said that an effective distribution of the network can strengthen it: The same is true of the distribution of legal powers and liability.

CONCLUSIVE REMARKS AND FUTURE WORK

It is easy to be fascinated by a new technology that has a bottom-up approach and seems to propose a viable alternative to an existing, and controversial, technology. But enthusiasm for this new "liberation technology" is often marred by the ambivalence of the political ideals that inspired it, an overestimation of the technical decentralisation achieved, or simply by a complete lack of any understanding of the legal sustainability of the proposed model. The multidisciplinary approach adopted in this research contributes to the expansion of the existing body of research on CNs and to the widening of our understanding of how political and cultural views and technical and infrastructural issues need to be continuously realigned and re-framed. The paper also shows how this ensemble of socio-technical elements has to be framed within both national and international regulatory and legal frameworks. Indeed, CNs provide an excellent example of bottom-up projects trying to subvert the physical architecture of the Internet itself, and the way this architecture takes shape is at the root of its very fragility. Researching the pressures and conditions of this fragility is a daunting task, since the structural weaknesses of a network are hidden at multiple levels, if not at the very intersection between potentially conflicting technical, social, cultural and political issues.

In this paper, we have given an in-depth description of the Ninux.org network, the largest Italian CN and one of the first to be created in Europe. Freedom to communicate and a decentralised infrastructure have clearly emerged as the core values of the Ninux.org project, which is seen as an

alternative to corporate and government exploitation of communication media for commercial and political ends. According to Ninux activist decentralisation and distribution of the network seem to be the key differences from mainstream providers that would guarantee the CN's development as an "alternative Internet". However, our technical analysis has shown that just "being distributed" does not guarantee that a CN is effectively different from a hierarchical, traditional network. We have shown that the mobilisation of activists and participants, when combined with the intrinsic difficulties related to the bottom-up construction of a network, does not automatically/necessarily generate an effectively decentralised infrastructure for Ninux.org. In fact, the network has evolved with inconsistencies that are not introduced "by design", as in traditional networks, but emerge spontaneously from the project. One such inconsistency is the fundamental role played by certain network nodes, another is the fact that discussions in the mailing lists are generally led by a small core group of people. Moreover, from a legal point of view, this concentration of responsibilities (despite being informal, and not explicitly assigned) weakens the network. Even though Ninux.org has no legal representative, it has a small set of people and nodes that could be the target of legal actions aimed at fracturing the community and discouraging its growth.

With regard to the technical aspect, CNs need to develop instruments that can monitor their evolution and verify that the network is achieving a satisfactory compromise between the goals that the community sets for itself and a manageable network infrastructure. Although this paper does not provide any solutions, we can suggest guidelines for future improvements, based on the enrichment of the technological instruments that Ninux.org uses (and other networks too). One suggestion would be the modification of the mapserver we described in Section 3, to show the following information: the centrality of nodes, which can be visually embedded in the map by changing the size of the nodes to reflect their centrality; and the ownership of nodes, which can be displayed with different colours. Since the mapserver is a key element in the management of the community, even introducing these simple features would draw the community's attention to the predominance of some nodes and members of the community. This would, in turn, make it easier to find solutions, such as the creation of nodes that decrease the importance of the critical ones (when possible), or the shared management of the existing nodes among more than one person in the community. As a further step, one can imagine periodically taking the "pulse" of the community with a survey on the network features, which could be sent to all community members. The survey would begin by giving the community new information about the network itself (its growth, the community's growth, etc.) in order to attract people`s interest; it would then ask questions like: what are user`s perceptions of the distribution of the ownership of nodes or the number of critical nodes? Evaluating the predominance of certain nodes might also increases the "legal sustainability" of the CN, as it would allow a more efficient distribution of responsibility and a better assessment of liability rules. Based on the answers to the survey, the community could set thresholds to express the level of satisfaction about the way the network was evolving, and provide input to initiate a discussion among the community participants about how to solve any issues that emerge.

More broadly, the picture that emerges from this multidisciplinary analysis of the Italian wireless CN Ninux.org is closely linked to the multidimensional factors that together have shaped the emergence of this alternative network. Indeed, the forms of members participation cannot be understood without reference to the actual infrastructure topology; at the same time, understanding the whole set of political assumptions supporting the project is crucial to the expansion of the CN, both in terms of participant numbers and of the network's physical growth; and finally, the potential legal liabilities to which these networks are exposed must be considered in any vision of the future development of the project.

ACKNOWLEDGMENTS

This work was financed partially by the University of Trento under the grant "Wireless Community Net-works: A Novel Techno-Legal Approach" – Strategic Projects 2014, and partially by the European Commission, H2020-ICT-2015 Programme, Grant Number 688768 "netCommons" (Network Infrastructure as Commons).

REFERENCES

Akyildiz, I. F. and W. Xudong. (2005). "A survey on wireless mesh networks". *Communications Magazine,* IEEE, 43(9): 23-30.

Antoniadis, P., B. Le Grand, A. Satsiou, L. Tassiulas, R. L. Aguiar, J. P. Barraca and S. Sargento. (2008). "Community Building over Neighborhood Wireless Mesh Networks". *Technology and Society Magazine,* IEEE, 27(1): 48-56.

Atton, C. (2001). Alternative Media. London: Sage.

Baig, R., R. Roca, L. Navarro and F. Freitag. (2015). "Guifi.Net: A Network Infrastructure Commons". *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development*. ACM, New York, USA, 27:1, doi:10.1145/2737856.2737900.

Baistrocchi, P. (2003). "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce". Santa Clara *Computer & High Technology Law Journal* 19(1): 111-130.

Beritelli, L. (ed.). (2012). +kaos. 10 anni di hacking e mediattivismo. Milano: Agenzia X.

Bird, C., A. Gourley, P. Devanbu, M. Gertz and A. Swaminathan. (2006). "Mining Email Social Networks". *Proceedings of the 2006 International Workshop on Mining Software Repositories*.

Brown, M. B. (2014). "Politicizing science: Conceptions of politics in science and technology studies". *Social Studies of Science* 45(1): 3-30.

Callon, M., P. Lascoumes and Y. Barthe. (2009). *Acting in An Uncertain World: An Essay on Technical Democracy*. Cambridge: MIT Press.

Carroll, J. M. and M. B. Rosson. (2003). "A trajectory for community networks". *The Information Society* 19(5): 381–393.

——— . (2008). "Theorizing mobility in community networks". *International Journal of Human-Computer Studies* 66: 944–962.

Chenou, J. M. (2014). “From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s”. *Globalizations* 11(2): 205-223.

Clement, A. (2014). “NSA Surveillance: Exploring the Geographies of Internet Interception”. *iConference 2014 Proceedings*. Pp. 412-425, doi:10.9776/14119.

De Filippi, P. and F. Tréguer. (2015). “Expanding the Internet Commons: The Subversive Potential of Wireless Community Networks”. *Journal of Peer Production* 6: 1-11.

Downing, J. D. (2000). *Radical media: Rebellious communication and social movements*. London: Sage.

Dulong de Rosnay, M. (2015). “Peer-to-peer as a Design Principle for Law: Distribute the Law”. *Journal of Peer Production* 6: 1-9.

Frangoudis, P. A., G. C. Polyzos and V. P. Kemerlis. (2011). “Wireless community networks: An alternative approach for nomadic broadband network access”. *IEEE Communications Magazine* 49: 206–213. doi:10.1109/MCOM.2011.5762819.

Giannone Codiglione, G. (2013). “Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi”. *Il diritto dell’informazione e dell’informatica* 28(1): 107-143.

Giovanella, F. (2014). “Wireless Community Networks: Inquadramento legislativo e questioni di responsabilità civile nel sistema italiano”. *Il diritto dell’informazione e dell’informatica* 29(6): 957-979.

——— (2015) “Liability issues in Wireless Community Networks”. *Journal of European Tort Law* 6(1): 49-68.

Latour, B. (2004). *Resembling the social*. Oxford: Oxford University Press.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. New York: Doubleday.

Liebowitz, S. J. and S. E. Margolis (1994) “Network Externality: An Uncommon Tragedy”. *Journal of Economic Perspectives* 8(2): 133-150.

Lievrouw, L. (2011). *Alternative and Activist New Media*. Cambridge: Polity.

Mac Síthigh, D. (2009). “Law In The Last Mile: Sharing Internet Access Through Wifi”. SCRIPTed 6(2): 355-376.

Maccari, L. (2013). “An analysis of the Ninux wireless community network”. Wireless and Mobile Computing, Networking and Communications (WiMob), *IEEE 9th International Conference*. Pp. 1-7.

Maccari, L. and R. Lo Cigno. (2015). “A week in the life of three large wireless community networks”. *Ad Hoc Networks* 24.

Maccari, L., L. Baldesi, R. Lo Cigno, J. Forcono and A. Caiazza. (2015). “Live Video Streaming for Community Networks, Experimenting with PeerStreamer on the Ninux Community”. *Workshop on Do-it-yourself Networking: an Interdisciplinary Approach*, ACM New York, NY, USA. Pp. 1-6.

McCaughey, M. and M. D. Ayers (eds.) (2004). *Cyberactivism: Online Activism in Theory and Practice*. New York: Routledge.

Milan, S. (2013). *Social Movements and Their Technologies: Wiring Social Change*. New York: Palgrave.

Orlikowski, W. (2007). “Sociomaterial Practices: Exploring Technology at Work”. *Organization Studies* 28(9): 1435-1448.

Oudshoorn, N. and T. Pinch. (2003). *How Users Matter: The Co-construction of Users and Technology*. Cambridge: MIT Press.

Page, W. H. and J. E. Lopatka. (2000). “Network Externalities”, in B. Bouckaert and G. DeGeest (eds.) *Encyclopedia of Law and Economics, Volume I. The History and Methodology of Law and Economics*. Cheltenham: Edward Elgar, Pp. 952-980.

Pascuzzi, G. (2010). *Il diritto dell’era digitale*. Bologna: Il Mulino.

Pasquinelli, M. (2002). *Media Activism. Strategie e pratiche della comunicazione indipendente*. Rome: Derive Approdi.

Pelizzoni, L. and M. Ylonen. (2012). *Neoliberalism and Technoscience: Critical Assessments*. Farnham, UK: Ashgate.

Powell, A. and L. S. Shade. (2006). “Going Wi-Fi in Canada: Municipal and community initiatives”. *Government Information Quarterly* 23(3-4): 381-403.

Robert, R., M. Manulis, F. De Villenfagne, D. Leroy, J. Jost, F. Koeune, C. Ker, J.M. Dinant, Y. Poullet, O. Bonaventure and J.J. Quisquater. (2008). “WiFi Roaming: Legal Implications and Security Constraints”. *International Journal of Law and Information Technology* 16(3): 205-241.

Schuler, D. (1994). “Community networks: Building a new participatory medium”. *Communications of the ACM* 37(1): 38-51.

Shaffer, G. (2011). “Banding together for bandwidth: An analysis of survey results from wireless community network participants”. *First Monday* 16(5).

Söderberg, J. (2010). “Reconstructivism versus critical theory of technology: Alternative perspectives on activism and institutional entrepreneurship in the Czech wireless community”. *Social Epistemology* 24(4): 239-262.

Söderberg, J. (2011). “Free Space Optics in the Czech Wireless Community: Shedding Some Light on the Role of Normativity for User-Initiated Innovations”. *Science, Technology & Human Values* 36(4): 423-450.

Tapia, A. H. and J. A. Ortiz. (2010). “Network hopes municipalities deploying wireless internet to increase civic engagement”. *Social Science Computer Review* 28(1): 93-117.

Verbiest, T., G. Spindler, G. M. Riccio and A. Van der Perre. (2007). Study on the Liability of Internet Intermediaries. Available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (accessed on 20 June 2015).

Wilson, S. (2015). “How to control the Internet: Comparative political implications of the Internet’s engineering”. *First Monday* 20(2). doi:10.5210/fm.v20i2.5228.

[i] See http://www.freifunk.net, http://www.awmn.net, http://www.guifi.net.
[ii] http://wiki.Ninux.org/Manifesto.
[iii] http://picopeer.net/PPA-en.html.
[iv] http://www.map.ninux.org.
[v] For the source code used in the analysis, see https://bitbucket.org/leonma/difffrom.
[vi] The metric is formally expressed as: Where P is the participation metric used in Figure 6 and O is the ownership metric used in Figure 4 normalised by the maximum value.
[vii] http://wiki.Ninux.org/GestioneIndirizzi.
[viii] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] Official Journal (OJ) L 178, 17.7.2000, 1–16.
[ix] See, for example, the terms and conditions of Telecom Italia, “General Contractual Clauses” for ADSL supply: Clause no. 7 provides that the access to the Internet through the ADSL cannot be granted to other users in a way that allow the latter to use the services linked to the Internet access (terms available at http://www.telecomitalia.it/sites/default/files/files/documentation/Condizioni_Gen_Contratto_Alice_0.pdf).
[x] The issue of “unsecured wi-fi” has already been resolved considering the Wi-Fi owner accountable for the conduct of third parties both in France and in Germany, even if only for cases of copyright infringement. See the German Federal Supreme Court (BGH) decision “Sommer unseres Lebens” (I ZR 121/08, 12.5.2010) and the French Intellectual Property Code art. L. 336-3, as amended by Art. 11, Loi n. 2009-669 of 12.06.2009, so called “HADOPI law”. In front of the European Court of Justice is currently pending a request for preliminary ruling by the Regional Court in Munich (LG München) asking for clarification on the liability of Wi-Fi operators (cf. McFadden C-484/14).

Stefano Crabu is at FISPPA Department, University of Padua

Federica Giovanella is at Faculty of Law, University of Trento

Leonardo Maccari is at Department of Information Engineering and Computer Science (DISI), University of Trento

Paolo Magaudda is at FISPPA Department, University of Padua

Journal of Peer Production - ISSN: 2213-5316