Hackivism, Infrastructures and Legal Frameworks in Community Networks: the Italian Case of Ninux.org

Leonardo Maccari
Department of Information Engineering
and Computer Science (DISI)
University of Trento
maccari@disi.unitn.it

Paolo Magaudda
FISPPA Department
University of Padua
paolo.magaudda@unipd.it

Stefano Crabu
FISPPA Department
University of Padua
stefano.crabu@gmail.com

Federica Giovanella
Faculty of Law,
University of Trento
federica.giovanella@unitn.it

Abstract:

Community Networks (CN) are an emerging world-wide phenomenon that caught a growing attention by a number of different disciplines. A CN is an infrastructure for digital communication alternative to commercial Internet Service Providers (ISPs) that resemble a scaled-down Internet, and is used to interconnect a community of people who share distinctive goals and identities. By developing a multidisciplinary gaze at the turn of science and technology studies, law and informatics, this paper analyses the cultural, technical and institutional dimension of Ninux.org, the largest Italian CN based on wireless technology and composed by more than 320 nodes mostly concentrated in Rome, but spread all over the country. The main contribution of the paper will be to unfold some of the main political, technical and legal issues of the Italian CN, highlighting how these different aspects result as strictly interwoven one with each other and can hardly be understood as separate dimensions. In doing so, the paper starts presenting a broader description of the phenomenon of CNs, sketching out its historical development, social motivations sustaining it, a basic technical description of its functioning and also main legal implications raised by these grass-roots alternative networks. Then, we focus specifically on the case of the Ninux.org CN, looking especially at practices, discourses, and interactions among activists participating in the project. On the basis of this analysis we move to consider some technical outcome of the network, highlighting how the technological infrastructure reflects or modifies initial intentions of the community, and especially how the issue of decentralization and horizontal organization of the network is only partially achieved on the technical ground. Moreover, we analyse some of the legal constraints due to the Italian and European normative framework in order to highlight how the development of Ninux needs to address regulatory issues in the near future. Finally, on the basis of this multi-perspective analysis of the Italian CN, the paper outlines some guidelines to enhance the community network, and to help its participants to develop reflexive tools to implement their initial goals of decentralization.

Keywords: Wireless community networks, Italy, hacktivism, distributed infrastructures, interdisciplinarity.

Introduction

The Internet is rushing towards its centralization. A few network operators, cloud, email and social network services, currently handle the large majority of the data exchanged on the whole Internet, and this has been used by regimes (Wilson 2015) and non-regimes (Clement 2014) to disconnect citizens or control their behaviour. While this state of things emerges more and more clearly, attempts to build *alternative Internets* take place, trying to subtract portions of people's traffic from the “black hole” that the Internet has become. Since the “Internet” is a mix of cables, routers, protocols and applications, efforts to build alternative communication models exist at any of the considered layers. Some well known examples are the Tor network, the Bitcoin distributed currency, or the Diaspora distributed social network. Those projects, not by chance, live in the software domain. It is indeed easier to program a new application that can compete with existent privacy-infringing platforms, than deploying a new physical network that can distract a significant portion of the Internet users from the Internet itself. Unfortunately, the rush to the centralization of services is strictly related with the physical architecture of the Internet and can not be overcome unless that architecture is subverted (or at least complemented). In spite of the inherent difficulties, there are people that nonetheless try to obtain this subversion: they are the subject of this paper.

In order to develop the study of the alternative forms of digital networks, we will analyse Ninux.org, an instance of what is called a *community network,* an Italian experiment to build an alternative physical network infrastructure. Community networks (CN for brevity) are infrastructures for digital communication alternative to commercial ISPs, that resemble a scaled-down Internet and that are used by a local community of people; while they can be set-up with different technologies, since the 2000s these alternative CNs have been primarily developed with wireless technology, so allowing to build these alternative networks in a simpler and less expensive way. CNs are blooming in many countries, with very different models: from small networks to cooperative ISPs made of tens of thousands of nodes. A CN is not only a network that interconnects a group of people, often a CN is an interconnected *community* of people, who share distinctive social and political ideas: usually CNs aim at realizing on a technical ground broader social and political goals and especially to build a fair, sustainable and more democratic communication infrastructure.

As it is common in other hacktivism practices, the original ideals and the concrete realizations may greatly differ. Indeed, creating a network infrastructure that is decentralized, more democratic and built on the premises of peer-to-peer interactions is a complex task. This paper investigates this complexity in the experience of the Italian WCN called Ninux, started in 2001 and developed especially in the last couple of years. Thus, we will explore discourses and politics developed within the Ninux community, analyzing how these cultural and social dimensions are effectively translated into the technical realization of the network, also looking at how CN’s political and technical practices fit into the national legal framework of digital communications.

The main contribution of this paper lies in a double goal. On the one hand, the paper will unfold some of the main political, technical and legal dimensions of the italian CN, highlighting how these different aspects result as strictly interwoven one with each other and can hardly be understood as separate issues. Inspired by Science & Technology Studies’ approach (Latour 2004) aimed at disentangling the articulation between the technical, the discursive and the social dimensions of socio-technical phenomena, the paper has the goal to displace alignments and differences that characterize technical, social and legal features of Ninux. Moreover, with this work of analysis we will also help the sustainability of CNs, that we intend as the mix of political and social engagement, its technical mediation and its relationships with the 'outer world' (and thus with the legal ecosystem).

On the other hand, and as a consequence of the previous point, the paper also wants to contribute to the development of a multidisciplinary framework for the study of CN and, more in general, of grassroots digital communication infrastructures. The research group that has carried out the research is indeed characterised by the interaction of several disciplines, including social sciences, computer engineering, and law; this heterogeneity is reflected in the distinct perspectives emerging along the

paper, in the multiple research methodologies adopted and in the variety of data presented. Here we want to stress the importance of the multidisciplinary approach we followed: singularly taken, none of the technical, social or legal analysis is sufficient to figure out the complexities surrounding CNs. It is pretty easy to be fascinated by a new technology, that has a bottom-up approach and seems to propose a viable alternative to some existing and problematic technology. But the enthusiasm for a new 'liberation technology' often clashes with the vagueness of the social motivations that started it, with the overestimation of the technical decentralization achieved, or simply, with the complete lack of any judgement of the legal sustainability of the proposed model. Thus, we believe that our multidisciplinary approach contributes in a novel way to expand existing research patterns to CNs and to widen the understanding of actual values and implications of CNs, in which the technical and social aspects are deeply intertwined and can not be isolated.

A multiperspective overview of CNs' development

CNs represent a multifaceted phenomenon, whose early stages emerged together with the initial development of the Internet, embodying the countercultural perspective on information technologies as well as the idea that Internet should became a liberating tool in the hand of people and not a governmental instrument of control. Indeed, historically, the early example of CN can be considered the "Memory Project" established in Berkeley in 1973, that embodied in its functions and services countercultural and democratic instances (see Levy 1984). n the 90s, CNs based on users' maintenance were already a relevant phenomenon, carrying a distinctive set of political and cultural assumptions about the role of communities participating to the networks, as in the case of the Seattle Community Network Project (Schuler 1994, p. 43). In this period, especially in the US, a generation of community networks was developed to sustain local communities, also by offering commercial and administrative services, for example in tourism and emergency management (Carroll & Rosson 2003; 2008). However, as argued by Tapia and Ortiz (2010), projects supporting these local networks, created at the municipal level, were frequently characterized by a "deterministic" approach and often they did not produce the awaited outcomes in terms of participation and democracy. In the 2000s, the diffusion of low-budget wireless technology permitted CN to emphasize the importance of establishing an autonomous hardware infrastructure, allowing the creation of small independent networks in both Europe and US (De Filippi and Treguer 2015), as in the case of the Italian community analysed in this paper.

What makes social implications of CN particularly significant is that these networks are realized thanks to groups of people developing a common project and sharing distinctive views about meanings and values of their work (Shaffer 2011; Söderberg 2011). Behind a community network we find, if not a "community" in a proper sociological sense, at least an effective working group, where participants present some degree of identification and involvement in the project, that is generally conducted on a voluntary basis with a variegate range of personal motivations and incentives to participate (Antoniadis et al. 2008). Moreover, in several cases, public or local institutions can be a support for CN, seeing these projects as experiments of civic participation or bottom-up solutions for digital divide issues (Powell and Shade 2006; Carroll & Rosson 2008). For all these reasons, social and cultural backgrounds of groups and participants represent very relevant dimensions in order to understand CNs, which could be superficially addressed from a purely technical and organizational perspective.

At least since the 2000's a fundamental set of political motivations emerged from the more explicit intersections between CN and new media hacktivism (Lievrouw 2011). Community networks as alternative new media projects represent the latest incarnation of a long historical tradition of oppositional and radical media, such as pirate radio in the 70s (Atton 2002; Downing 2000). From this point of view, motivations for building CNs are directly linked with emerging political practices connected with critical views about informatics, software and the use of the Internet. Particularly after the Snowden's scandal in 2012 and the mainstream visibility gained by Anonymous cyber-political actions, public concern about Internet privacy and control greatly expanded, thus turning CNs - especially wireless ones - into a strategic topic within the political agenda of countercultural and social movements

(Milan 2013; De Filippi and Treguer 2015). As it has been argued by Söderberg (2010; 2011) focusing on the Czech Wireless network community, the sharing of a political view represents a key factor for participating in CN projects. In addition, the author also showed that despite political perspectives are fundamental, they are not static and take-for-granted frames; rather, it is important to consider that political views of participants in CNs are constantly negotiated and redefined, for example when market opportunities became an option to be considered. The crucial role played by political and normative perspectives shared by participants in CN highlight the importance of the analysis of cultural frameworks and collective motivations for the understanding of these networks dynamics and diffusion.

While political instances have played a pivotal role in the start of many of these projects, a crucial problem for the further development of CNs has been to scale over activist and computer geeks. Of course, networks that also provide Internet access in competition with ISP usually attract a larger number of people, while networks that do not offer that feature are less appealing to the general non-*geek* public. It is important to note that the size of the network does matter, since the larger is the network the higher is the chance that people are close enough to an existing node to have both the possibility and the will to join and to gain an advantage from the participation into the network, somehow resembling the economic concept of “network effect” (Liebowitz & Margolis 1994; Page & Lopatka 2000): basically, a large network grows faster than a small one. But on the other side it is also true that when the goal of the CN is to access the Internet, most of the benefits of its use will be limited to the overcoming of digital divide; there are few advantages in using a distributed and privacy aware-network to finally access Facebook. Indeed one unsolved dichotomy that is present in CNs is that it is easier to let a network grow when it becomes a cooperative ISP, but a local-only network has a higher (and still undeveloped) social potential (Maccari et al. 2015b).

Moving on to the main technical features of the CN, we can say that it is an instance of those that, in technical jargon, are called *wireless mesh networks* or simply *mesh networks*. A mesh network is a type of network in which there is no central element that mediates the communication, and the network evolution is spontaneous and unplanned. There is a large technical literature describing mesh networks (Akyildiz 2005); in this paper we will give an overview of the technical ground on which the network are built, that is essential to understand their potential social impact. Consider a common home wireless networks, it is based on an access point (AP) configured to be the centre of a star topology, all client devices that want to exchange data need to be connected to the AP and communicate through the AP, even if they are close enough to be able to communicate directly. The AP is connected to the Internet, and clients can access the Internet though the AP.

In a mesh network instead, there is no star topology, when two nodes are in direct communication range they simply exchange data via the wireless channel. The fundamental difference between the two configurations lies in the fact that while in a star topology the AP is more important than the others, in a mesh network all the nodes of the network are peer nodes, there are no more 'AP' and 'clients', just network nodes. In a star network, if the AP is powered off, the rest of the nodes can no longer communicate, while in a mesh network, as long as two nodes are within communication range they can always exchange data. A natural evolution of a mesh network is a multi-hop mesh network, in which communication between two nodes can 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 is routed from an intermediate node C, which behaves exactly like the routers that constitute the Internet. Figure 1 represents a schematic mesh networks mounted on rooftops.

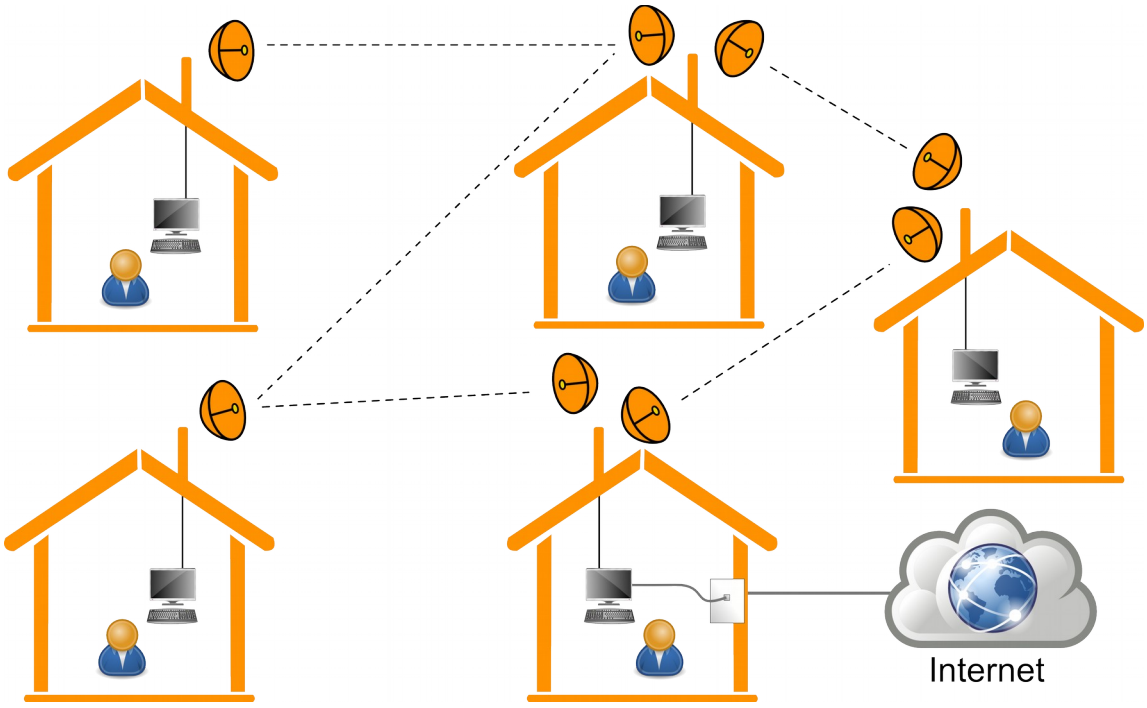

Figure 1: An example of mesh networks with antennas placed on rooftops

Such network does not require planning. To join the network a new node needs to have a line-of-sight connection with at least one of the nodes in the network. In turn, it will behave as the entry point for new nodes that come after him. In this way the network extends in an organic manner, without the need of a planning. Moreover, the network is self-organizing. Network protocols are made so that adding or removing nodes does not require reconfiguration on the already running ones. Again, if node C is a intermediary between node A and B and it is removed, the network protocols will take care or redirecting the traffic from A to B through another path, if it exists. Finally, the network is resilient. Because of the previous feature, the network resists to the failures of some nodes of the network. The more nodes compose the network, the less each single node is important in the global economy of the network. Of course, these benefits come at a price, that is the greater complexity in the network internals: it is intuitive to understand that it is easier to organize a network having a unique machine that controls the others, rather than a set of peer nodes that must reconfigure collaboratively at each change of the network topology.

In a CN, people install on roofs or terraces low cost wireless equipment (the price of the device alone can range from about 30 to 100 Euros, plus the cost of the mounting) that allows to create wireless links with other people. A CN is to all effects, a small Internet. People who participate can install their own servers and host services accessible by all other members of the community within the network. Among these services there are normally telephony, chat services, file exchange, social networking. The limit is given only by the personal initiative of the individual user.

In the figure 1, one of the nodes of the Community network is connected to the Internet. For this to happen, some users share their Internet connection with the rest of the network, functioning as gateways. Other users will reach the gateway via the CN and from there access the Internet. In some CNs there is no Internet connection, or it is based only on the initiative of the individual, in others, there are associations or real ISPs that play the role of the Internet gateway. Mesh networks have been largely studied as a last-mile replacement for Internet access (Baig 2015, Frangoudis 2011), in this paper instead we focus on their role as networking infrastructure for local communications.

Technologically, a CN offers some interesting features: the first is that the capacity of the links can be very high. Using affordable outdoor devices with directional antennas (similar to small satellite dishes), one can set-up wireless links that offer a throughput up to hundreds of megabits per second (the IEEE 802.11n standard achieves up to 300Mbps). In addition to speed, the traffic within the network suffers from minor delays compared to cable or DSL connections. This factor is particularly important

when using real-time services such as voice or video transmission. In addition, wireless links have symmetric performances, contrarily to ADSL connections there is no specific technological provision that imposes to have a larger download bandwidth than upload bandwidth. Using only low-cost devices links can be created that cover distances up to 20-25 kilometres when using directional antennas, such distances allow to build city-wide networks, with the limitation that a line-of-sight connection (no obstacles in between) is required. Finally, the communications remain local. On the Internet, the path to destination can include routers belonging to different legal entities in foreign countries. In Community networks the data remains in the local infrastructure.

The technical features of CNs make them different from the Internet, with regard to local communications. First of all, the network can not be easily switched off. As long as there is a path from the source to the destination, the communication can take place. When the network grows, there is no single point of failure introduced by design, so there is no “kill switch” that can be used to disconnect the participants. 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, to filter or to control in general. Moreover, in many cases there is no single entity that owns the network, so there is no single person that can receive the order to switch down or censor the network. These are attributes of generic distributed networks, which theoretically apply also to CNs. In the rest of the paper we will discuss how much this is effectively true.

Another key difference between CNs and the Internet is that the availability of symmetric bandwidth does not necessarily encourage the creation of centralized services. As mentioned, ADSL lines are made so it is faster to “download” rather than to “upload” the same content, thus it is more convenient to use a remote cloud service rather than hosting one at home. A simple example: when Alice wants to share a file with Bob and Eve, a direct transfer with a peer-to-peer protocol would use the slow upload connection twice. Instead, uploading it to a cloud service would use the upload connection once, and then any person that wants to access it will use their fast download connection. This example shows that asymmetric bandwidth, which is a limitation imposed by business models and not by technology itself, hinders the development of peer-to-peer services. Under this point of view, the realization of alternative networks whose characteristics are decided by the community and not by the market, represents a new way to revive the interest in peer-to-peer architectures.

The way CNs are structured might also be linked to the legal framework in which they develop: regulation can be either a tool to foster and reinforce CNs or an hurdle that hinders their prosperity. Under 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). CNs’ main hurdle for legal analysis lies in their technical and organisational architecture, which constitutes a barrier for the application of classical legal tools, such as civil liability (Dulong de Rosnay 2015, Giovanella 2015). Indeed, while some CNs are part of bigger projects such as foundations or associations, some others are just the result of a genuine spontaneous movement among the members of a community (De Filippi & Treguer 2015, pp. 3-4). In this latter case, CNs’ bottom-up approach is often reflected in the absence of a hierarchical structure and, most important, in the inexistence of a central administrative body with control or representative powers. This implies the lack of legal personality, that, in turn, means the impossibility to ascribe the liability to the network as such (Giovanella 2015, pp. 59 ff.).

Parallel to these peculiarities of the network’s structure, also the internal functioning of the community entails legal implications. For instance, the high level of anonymity, enhanced by the absence of databases on users’ information – including Internet Protocol addresses, is of great value for CNs and it implies a big potential for freedom of speech. However, it also impairs the possibility to enforce rights violated both within and outside the network (Dulong de Rosnay 2015, pp. 3-4; Giovanella 2015, pp. 54 ff.).

1 Birth and key developments of the italian CN Ninux.org

The case of Ninux.org is part of a recent revival in the development of community network across the European region. Thanks to wireless technology, in the last decade we witnessed to the birth of several projects aimed at building grassroots community networks, based on communities of activists and driven

by different needs and demands (Defilippi and Treuger 2015; Shaffer 2011). For instance, among most important European CNs we have freiFunk in Germany, AWMN in Greece, and Guifi.net in Spain[1]. The latter, started in the region of Catalunia in 2004, is the biggest of the region, being currently participated by more 80.000 users, who are mainly attracted by the possibility to obtain Internet access independently from commercial ISP. Other networks, such as freifunk in Germany and Wlan Slovenija, did not develop primarily as concurrent of traditional commercial ISPs, but originated mainly from political activism around the importance of decentralized networks in digital society. In these last cases, while the ideological drive represented the initial input, communities needed to offer to users convenient services in order to scale the narrow niche represented by media activists or experts (Defilippi and Treuger 2015, p. 6).

The Italian project for a wireless community network started originally in Rome, but expanded especially in the last few years adopting the name of Ninux.org, which identifies a national platform gathering the several independent urban-based "islands" involved. The most important and larger urban network remains the one raised in Rome, where the majority of the about 330 national active "nodes" of the network are located (see Maccari 2013). The origin of the project goes back to 2001 in Rome, where a group of students and hackers started experimenting with grassroots wireless networking following the recent example of Seattle Wireless, created in 2000. As few 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); this decrease in costs soon permitted an increase of the individual antennas installed above the roofs of participants and their friends. The "island" of Rome served as an example for the development of other local wireless networks in other Italian cities, such as Florence, Bologna, and Pisa in the North, and Cosenza in the South. While the infrastructure in Rome has achieved a significant number of "nodes" and has become a functional network for hundreds of people, the other "islands" still remain in an experimental stage with networks that have not yet scaled to larger dimensions than the core group of experts and activists.

Even if the local "islands" share a common general technical and political framework, they developed independently in terms of connectivity and organization, and their respective working groups are driven by distinctive mixes of needs and motivations, at the same time political, technical and locally concerned. For example, while Ninux still remain an informal and not institutionalized entity, some of the "islands" have established some kind of indirect relationships with institutional actors, such local institutions, ISPs or universities. Moreover, some "islands" are moved primarily by political concerns, which turn out to structure more solid ideological frameworks in their structure; other "islands", although they also share strong political drives, they are not *a priori* against the inclusion of market processes within the building of their networks. Therefore, while moving from similar backgrounds and political sensibilities, every city is characterized by a slightly different set of cultural background and degree of political mobilization. In the case of the "island" of Pisa, participants are strictly interconnected with student leftist associations as well as with squatted "*centri sociali*". In Florence, key participants to the network came from previous experiences of media activism, including the participation to the open software movement. Activists of the smaller network in Bologna are a mix of technology enthusiasts, often enrolled as students at the local University, and activists of a squatted "*centro sociale"* in town.

Although independent from each other, all these networks are part of the wider national project named Ninux.org, which represents a common working platform for all the participants. Rome and groups in other cities directly involved into the project share a common vision on the role of CNs in society and on the general ways these networks should develop. This common view has been negotiated collectively and is exposed in a "Manifesto" available on the project's web site[2], each participant of Ninux.org is the owner of its node, and has to agree the Ninux manifesto which is largely based on the Pico Peering Agreement[3] that several other international CNs apply. Major features highlighted in this document cover several aspects, which reflect the heterogeneity of the dimensions raised by the projects, including: the crucial importance of the technical choice to go for decentralised

[1] see www.freifunk.net, www.awmn.net, www.guifi.net

[2] http://wiki.Ninux.org/Manifesto

[3] http://picopeer.net/PPA-en.html

and mesh architectures; the role of CN as a democratizing tool and as a resource to fight digital divide; its connections with the issues regarding the freedom of expression; a criticism toward the influences by commercial pressures. These several instances reflect the whole set of needs, motivations and political drivers that sustain discourses and practices of the Italian wireless community network context.

Finally, a focal aspect that needs to be highlighted concerns the forms of digital communication adopted by the CN's activists. Currently, the mailing lists used by the different islands that constitute Ninux.org represent an important instrument of coordination and collaboration, which accompanies face-to-face meetings. Generally, each single island predisposes its specific mailing list, to which any members may sign up, to participate in the ongoing discussions. In this context, the mailing list identifies a communication device for sharing of meetings minutes, proposals of technical solutions to be implemented, ongoing technical problems to be fixed, and information regarding national and international events which may be of interest for the community. These contents constitute core elements for the management of the community. For this reason Ninux.org's members archive in a website accessible to anyone, and anytime all communications which occurred in the mailing lists, thereby shaping a digital collective memory related to the construction processes of the CN.

2 Politics and discourses in the Ninux.org commuity

In this section we concentrate on the ways the Italian community network embodies specific political motivations, and how these motivations intersects with the technical evolution of the network. In doing so, we ground these reflections on an STS (Science & Technologies Studies) perspective, which allows to study the constitutive entanglement of the social, the political and the technological in different settings and situations (see Callon, Lascoumes & Barthe 2009; Brown 2014). This theoretical tradition allows to put on the foreground that technical dimensions of CNs are strictly connected and intertwined with political and cultural frames shared by activists. Moreover, this perspective also enable us to unfold the peculiar tensions and negotiations between technological aspects and the political claims connected to a critique of the evolution of the Internet governance, and of networking technologies in general (McCaughey & Ayers 2004).

An initial point is that, while the majority of Ninux.org's members believe that CNs identify an informal organization without strong ties to specific political traditions, it's important to stress that many symbolic and discursive elements shared by CN activists are part of a broader Italian antagonist movements focused on ICT (Pasquinelli 2002; Beritelli 2012). These political instances got relevance especially since the anti-G8 movement in 2001, which helped to reinforce a “hackmeeting” movement, and the spread of informatics-based antagonist activities within the plethora of squatted social centers around the country.

Genealogically, the community of Ninux.org represents a socio-technical context in which are located experimentation and innovation activities connected with ICT. First of all, to trace an analysis of the different logics of participation to the project, we can refer to the utterance of one of the most active member, according to which:

> 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 CN circumscribe a collaborative space within which members collectively share a passion concerning a set of activities related to the manipulation of devices and technological equipment which, ultimately, allow the building of wireless infrastructure. From an organizational standpoint, the CN gathers a group of people who share the same interest in the possibility of shaping a specific technoscientific 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 & Pinch, 2003).

Participation to the Italian CN is rooted in and juxtaposed with cultural frameworks, densely connected by political aspirations and claims concerning the critical use and the appropriation of ICT. In this context, the political side should be considered as a driver of practices of constructing an alternative to the infrastructures' global governance for digital communication, which is more and more shaped by a ‘neo-liberal paradigm’ (Chenou, 2014; Pelizzoni & Ylonen 2012). The predominant feature of the political dimension of Ninux.org community regards the critique of the contemporary global strategies of organization and governance of the Internet, which can be defined in terms of a ‘cyber-governance’. This concept states the juxtaposition between technological, scientific and legal devices through which the regulation architecture of the relationships between social actors and the Internet infrastructure is articulated, also in its proprietary borders, contents, modalities of services access, and participation. Indeed, the centrality of the critique to the current cyber-governance is a constitutive and transversal theme to the narrations of the members' participation to the CN:

> Just the fact that someone says: "Sorry, but Internet is not already at 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, now it is growing, 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's 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 discloses a specific political positioning, which is highly pervasive in sustaining collective action and participation: the Internet is not considered by Ninux activists as a neutral tool for digital communication, but it is rather conceived as an infrastructure permeated by peculiar negative functional logics which should be hindered. Among these negative aspects are the centralization 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 aspect called into question by community networks as Ninux.org relates less to the technological dimension itself, and more to the way that shaping an infrastructure is strategic to call into question Internet's cyber-governance. In this sense, a distributed infrastructure represents a translation of political visions into a material network aimed to cultivate and sustain practices of cyber-resistance, through which innovative conceptions of the relationship between citizens and communication technologies are emerging.

However, while political motivations are widely shared and are the basis of a common identity within the project, there is not a cohesive view on the way these political stances can be arranged with technical choices and targets. This has been particularly evident when comparing smaller and more politicized local ‘islands’, such as Florence or Pisa, with the trajectory of the larger Ninux local community in Rome.

During our empirical research, these political motivations have been particularly emphasized by several activists of local contexts where the project Ninux.org is still emerging, such as those from Pisa, Bologna and Florence. On the other side, the gradual extension of the network in Rome has been a source of contradictions with regard to the level of the political aspirations, and this may undermine the practices of technological experimentation, to the advantage of management and maintenance of the infrastructure. More precisely, the relationship between technological experimentation activities and the need to ensure stability to a large distributed infrastructure, can shape a conflictual pluralization of the visions concerning the way in which the community network should be realized. In this regard, it is useful to focus on the following thoughts from a veteran activists of the Ninux.org in Rome:

> *Long time ago, people who start 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 became 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 points out that the relations between activists, political aspirations and technologies can shape a conflictual socio-technical space, which can be connoted by tensions, and recursive negotiations on the boundaries between the implementation of consolidated knowledge (which already work), and the push to experimentation and creation of new skills and knowledge capable of translating political aspirations into an alternative network which embeds new conceptions on the use of ICT. From these considerations, Ninux.org appears not as a fully coherent and cohesive technical and political project, but rather as the result of a plurality of visions, sometimes even conflicting one with each other, such in the case when technical reliability and efficiency of network is opposed to the work of continuous experimentation.

Overall, this section has highlighted how the “political dimension” represents a crucial element in fostering the construction and sustainability of distributed CN. At the same time, it is not a monolithic vision, but rather a discursive context of debate locally articulated, and constantly re-negotiated by the participants during the activities of construction of the community network. In this sense, technical analyses and assessment of these networks should consider more and more the political cultures of the local contexts in which distributed networks are developed.

3 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 criticism of the current organization of the Internet, its governance, and the predominance of a service model in which the user gives away any control on the instrument he 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 is governed with a peer-to-peer approach. In this section we will describe an analysis we have carried out to verify how much of this initial spirit that animates the community is effectively translated into the realization of the network, and the interactions in the community.

Figure 2 reports a snapshot of the current topology of Ninux in Rome taken from the *mapserver* in the Ninux.org website[4]. The mapserver represents a key asset of the Ninux community, and of many more communities, when a new member wants to join the community, he enters his position in the mapserver and creates a “potential” node, that is a placeholder which expresses his interest in joining the community. From there he can be contacted by other people that have nodes nearby and join the network. When a node passes from the “potential” to the “running” state it means it was physically installed and connected to the rest of the network, in that moment he actually becomes part of the network. We had access to the database populated with all the nodes, their links, and the owners of each node for Ninux. 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 considered only the largest component of the graph, that is the Rome Island, and, after aggregating nodes placed in the same location we extracted a graph made of 140 nodes and 158 edges. We will omit many details of the data collection that can be found, together with the source code and the data-set, in past works (Maccari et al. 2015).

[4] www.map.ninux.org

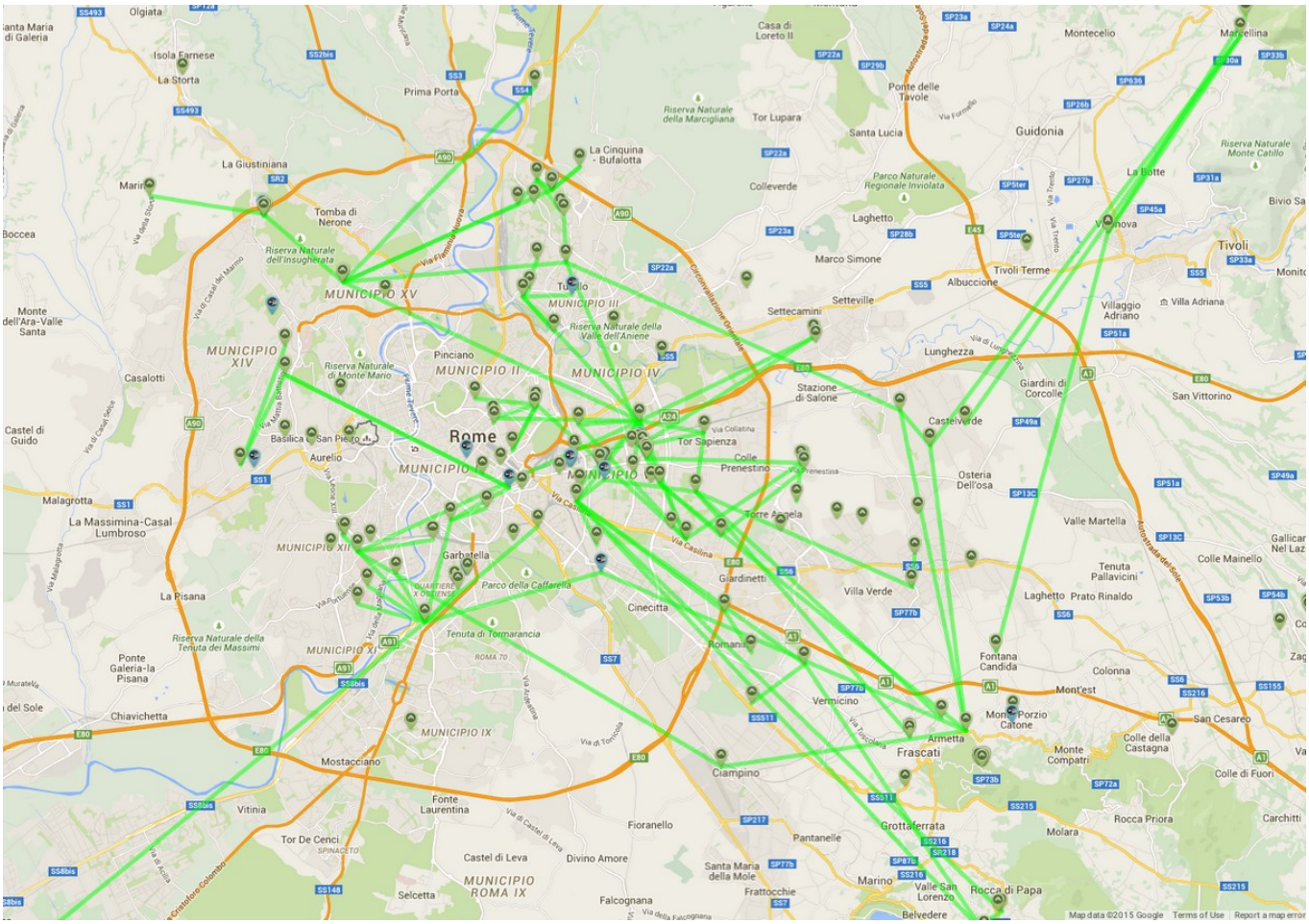

Figure 2: The current topology of the Rome Ninux network.

Our goal was to perform a technical analysis of the network graph to outline some criticalities and correlate them with the data regarding the structure of and participation to the network infrastructure. For this reason on the graph we computed three metrics that will complement the qualitative analysis we described so far and help us understand how much the network can effectively be considered “distributed”. These three indices are: the group betweenness, the ownership distribution of nodes and the ‘owner betweenness’. The group-betweenness approximates how much traffic passes through a group of nodes, and can be applied to any graph, such as a communication network or a road map. More precisely, to compute the betweenness of a node *k* one has to consider all the possible couples 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 will follow when node *i* communicates with node *j*. The betweenness of node *k* is the number of shortest paths that include *k*, normalized 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 those nodes may be able to intercept. We can also reverse the point of view. Let us suppose that an attacker wants to intercept the highest portion of traffic in the network, and to do that he is able to attack and control only a limited number of nodes: the group *K* with the highest group betweenness is the most suitable to accomplish this task. We computed the group with the highest betweenness for groups of size from 1 to 5, and we report it in figure 3.

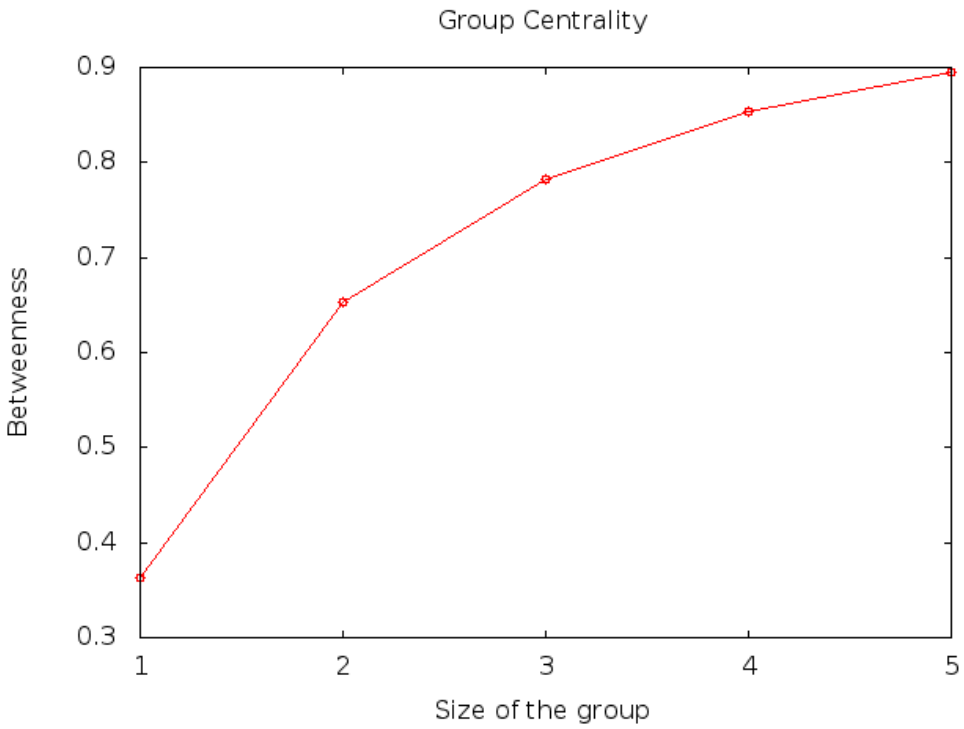

Figure 3: Group centrality in Ninux

Figure 3 shows that if an attacker is able to choose only 5 nodes over 140 in Ninux, he can actually access almost 90% of the whole generated traffic. We have observed this behaviour even in larger CNs (Maccari et al. 2015) and this actually shows that the sole fact of being "distributed" does not at all guarantee that there are no critical nodes in the network. Indeed, the control of a very small fraction of them allows to spy on the majority of the traffic. This is probably due to the model in which a network is built. Normally a CN starts with a few small disconnected islands inside a city, that become connected when a new node is placed in a dominating position (a hill, a tall building etc.). That node suddenly starts routing a large portion of the traffic, and for this reason, the community starts investing in its infrastructure, for instance adding new radios. This of course makes it even easier to connect to the node, and creates a loop in which the community invests a lot of effort in a few important nodes, and unconsciously re-creates 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 single person. In the node database to each node is associated a contact email, and we aggregated the nodes corresponding to similar emails using standard comparison procedures (Bird 2006) and human checking, even if there is room for some potential errors, the trend we will describe is clear[5].

[5] For the source code used in the analysis, see https://bitbucket.org/leonma/difffrom

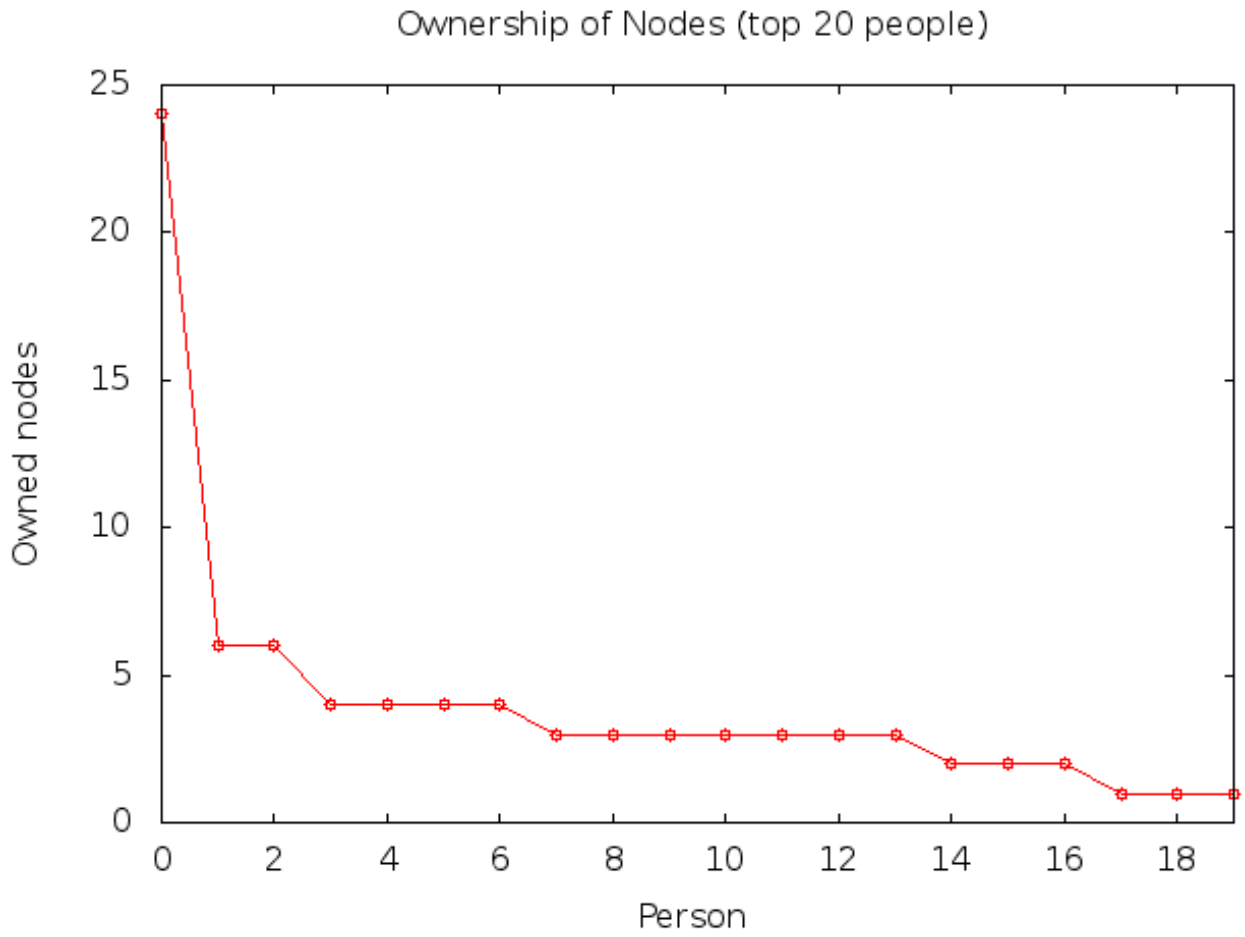

Figure 4: Distribution of nodes owned by a single person.

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

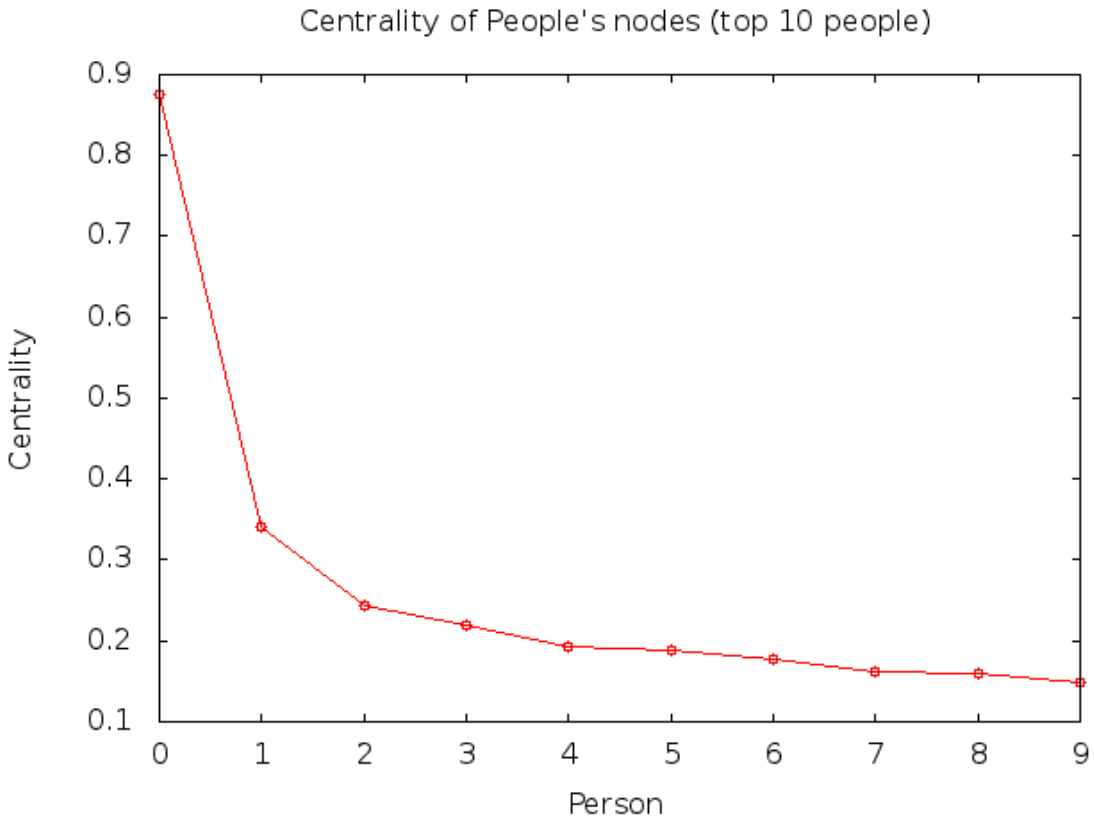

Figure 5: Centrality of the nodes owned by a single person

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 owns. Unsurprisingly the graph shows that there is a small group of people (and one in particular, that corresponds to the top owner of nodes) that could easily intercept a non-negligible amount of traffic. Again, a spontaneous attitude from the most skilled and collaborative people in the community creates 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 about one year of discussion and shows the normalized number of answered email per person. This is a very basic metric to determine how influential is a person in a mailing list, the rationale behind this metric is that the more answers a person receives to his email the more he is able to raise interest in his topics. Since it is a very rough metric we will not push into the interpretation, but again just outline the trend that clearly emerges.

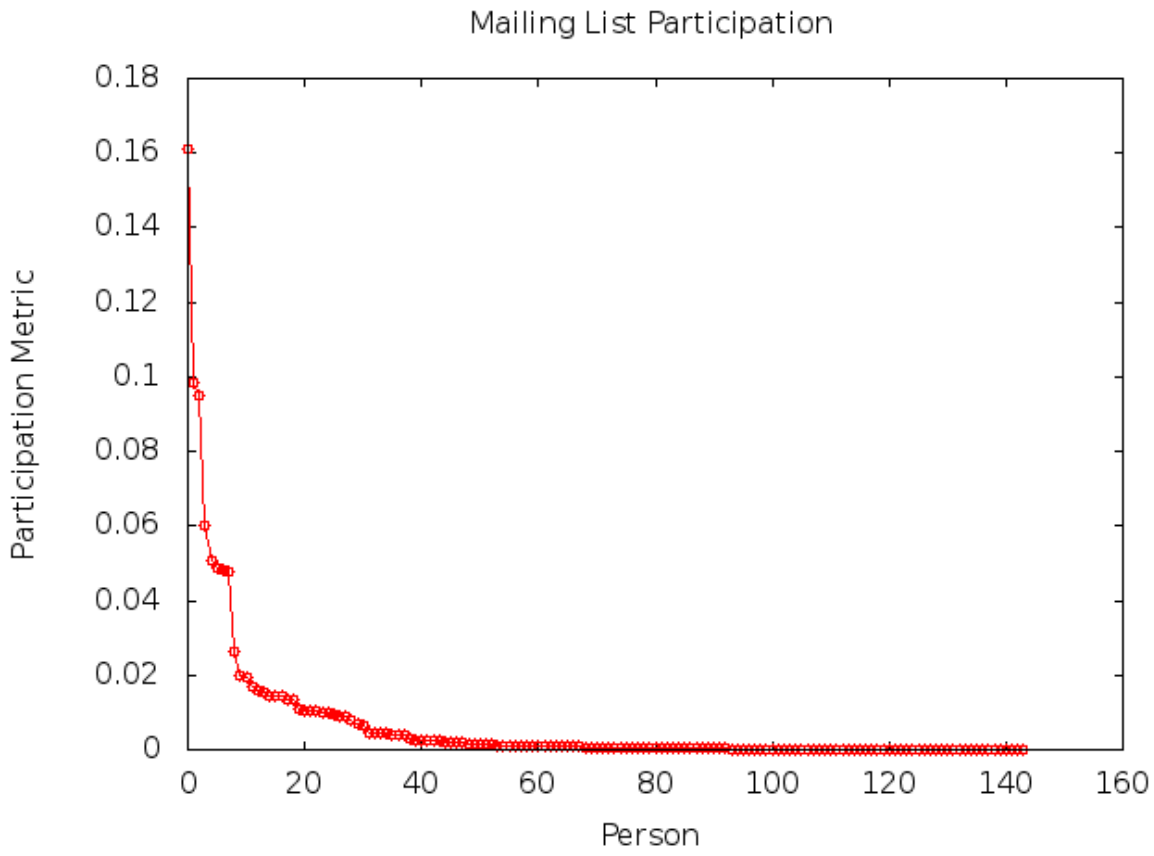

Figure 6: Number of answered email per person.

Figure 6 shows that the mailing list seems to be dominated by a few individuals, that monopolize the discussion in the mailing list. We wanted to understand if there is a correlation between ownership of nodes and mailing list activity, and we observed that such correlation exists. For each person we introduce a combined metric that takes into account both the quantities. [6]

We obtain the following graph:

[6]The metric is formally expressed as:

$$\gamma = 0.5 * P + 0.5 * \frac{O}{max(O)}$$

Where P is the participation metric used in graph 6 and O is the ownership metric used in graph 4 normalized by the maximum value.

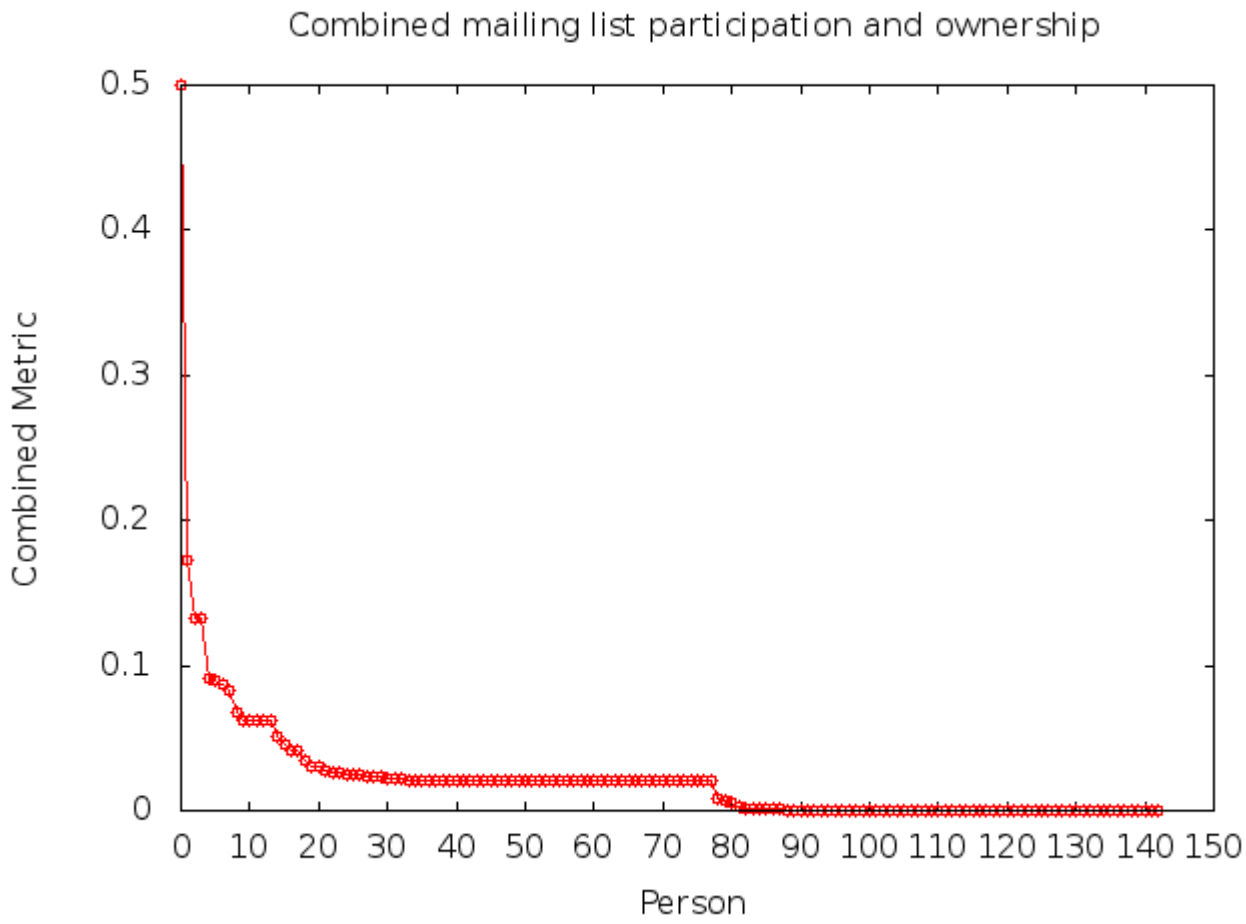

Figure 7: Combined participation and ownership metric

Which is, again, very skewed towards the high values, effectively showing that among all the people that write in the mailing list or own at least a node there is a small fraction that actively participate and a large number that marginally contribute to the community.

The data we analysed so far show that, despite the intentions of the community to create a network that is decentralized, community-managed and that offers some protection against intrusion, the implementation diverges from the original intentions. The network is pretty concentrated (as few as 5 nodes could in principle intercept 90% of the traffic), the ownership of the nodes has a skewed distribution, and the participation to the discussion mailing list is, again, concentrated on a few individuals. The reasons for this are to be looked in the spontaneous development process of the network, in which there are a few people that are really active and lead the discussion and the practical development of the network. We believe this is not a singularity of Ninux but can be observed also in other networks (the same topological features have been found also in other two community networks (Maccari et al.2015)), since it is a product of the spontaneous growth of the network. In other words, the fact that the network is unplanned does not necessarily facilitate the development of the network practice towards a real decentralized architecture.

This quantitative trend concerning the hierarchization of the discussion in the mailing list can be understood as an emerging outcome of a wider process - that involves the degree of motivation to devote time to the project, and other heterogeneous capabilities, such as technical and coordination skills- through which Ninux.org's members develop and elaborate their reputation, membership, roles, and authority within the community. The high centralization in the participation to the mailing list also emerges from a reading of the discussions' content that are activated in this digital communication space. Specifically, the most active members in the mailing list appear as a niche of activists to whom it has been informally "delegated" the task of introducing and coordinating the core and decisive discussions regarding the strategies of management, maintenance and development of the

infrastructure. From an analytical point of view the technical skills required to sustain this discussion and the management of the network are not horizontally spread, thus shaping the polarization of the "decisions making" concerning the management of the community. In this sense, the centrality of few activists in the coordination of technical maintenance and management of the infrastructure is also reflected in the vertical participation to the mailing list discussions, within which the discourse and management framework that support the CN is defined.

As contradictory as it can seem, to keep a high level of distribution in a decentralized network and its community, some coordination and monitoring is necessary, as we will suggest in the conclusions.

4 Ninux within the Italian legal framework

One of the first questions jurists usually pose when facing new technologies is about their legality, which is a key element to understand if and how that technology will have the chance to evolve and prosper. Moreover, with the legal analysis we want to shed some light on the concrete possibility that Ninux could be the target of some legal actions, that might represent another point of failure for the CN.

The present Italian framework for electronic communications (Electronic Communications Code: d.lgs. 1.8.2003, n. 259, as amended), which derives, for the greatest part, from EU law, allows the creation and diffusion of Wireless Community Networks (as Ninux.org) without the need of any authorisations. Indeed, the technologies on which CNs rely are considered as free activities (Giovanella 2014, pp. 960 ff.) and the implementation of CN is to be considered if not fully legal at least not explicitly prohibited. While in the past, the Italian legislation impeded the flourishing of these community, the current framework does not impair CNs' diffusion.

Under civil liability rules, taking into account the different subjects of CNs, three main liability situations can be imagined (Giovanella, 2015). First, a user could personally commit an illicit action within the network, and would consequently be liable for her own conduct on the base of the general rules of civil liability (i.e., for the Italian context, art. 2043 of the Civil Code). The first step to enforce a violated right would be to identify the alleged infringer. But this result may be very difficult to achieve. In Ninux there are no designated identification numbers: each user has an IP address but every peer chooses her own number that can be changed over time. In addition, there are no databases in which these numbers are registered: within the Ninux website there is a table collecting the IP numbers that each user chooses. Despite this rough database seems to provide important information to trace back IPs to real identities[7], the table is actually easily modifiable and falsifiable and cannot be considered a reliable tool under this point of view. Therefore, the possibility of identifying the wrongdoer intensely decreases. The problem persists in the case of a user routing someone else's illicit data; even in this instance no user can be identified and, consequently, considered liable.

A second possibility is that the illicit action starts from the network but it is directed outside the network, through a gateway. The gateway node can be identified since it has a public IP address, the gateway's provider could then match the access data with the identification data of its customer, obtaining the real identity of the gateway subject. Moreover, 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" would apply[8]. The Directive regulates the liability of providers for third party civil wrongs. Under the Directive, if ISPs comply with the specific conducts prescribed by the law, they will not be held liable for a third party's conduct (Baistrocchi 2003; Verbiest et al. 2007). The Directive divides ISPs' activities into three different categories: mere conduit, caching, and hosting (arts. 12-14). The Italian *verbatim* implementation of the Directive was made 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 offer only a connection to the Web are to be considered as 'mere-conduit' providers. This kind of provider seem the most important

[7] http://wiki.Ninux.org/GestioneIndirizzi

[8] 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.

for what it is here analyzed. Between the ISP providing connection and its customer there is a binding contract: a provider could limit its responsibility by means of specific contractual provisions, expressly forbidding the customer to share the connection. Contractual provisions of this kind already exist in various contracts[9]. In such cases, the customer/node-owner that opens her node to other 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, p. 107; Mac Síthigh 2009, p.366-369; Robert et al. 2008, pp. 217 ff.). This imposition of liability on the single customer or user could be a deterrent against sharing her connection with unknown or unreliable users[10]. More generally, this might represent a deterrent against opening the CN to the Internet.

This observation can be directly connected to the technical analysis we carried on, because in case the gateway node was one of the few critical ones on which the network relies, such a scenario might constitute a danger for the network's stability and robustness. If the most important nodes (i.e. those that vehiculate more traffic and that 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 the active involvement of people, it is advisable to separate gateway nodes (and their owners) from critical nodes in the topology (and their owners).

As a the third possibility, the same CNs might be considered as accountable entities. In case the bottom-up approach reflects into a total absence of an organizational structure, no legal personality exists and CNs cannot be sued. On the contrary, if a CN is organized as an association, specific liability regimes apply (i.e. 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 the actions of the members. This would also entail some consequences in terms of being more controllable.

The choice of a CN about whether to organize itself as an association can in fact bring both positive and negative effects. Among positive effects one can easily think to the possibility of obtaining public and private subsidies. Moreover, a formalization of the network could help in those cases where the network could function as a - broadly speaking - lobbyist. As for negative effects, we shall consider the need to organize the governance of the network and distribute the accountability among some of the members; this could stiffen the structure of the network, that could partly loose its "genuineness". In addition, based on the empirical analysis illustrated in Section 3, it is plausible that organisational roles would be assumed by the same people who proved to be critical for the life of the network. These people are indeed the most interactive, the most involved, and those who care most for the health and the survival of the network. Therefore it could be natural for these people to take on organizational and accountable roles in a possible network-association. Under a certain point of view this overlap might be desirable: as the analysis conducted illustrates, some coordination is necessary if the network wants to keep and rely on a strong decentralization. If critical nodes' owners were also those having organizational roles, the entire network could be more easily coordinated and monitored. But at the same time this could constitute a danger for the stability and the robustness of the network and for its sustainability. Let us suppose that the association was sued; one of the person in charge of the association would represent the entire network and might be considered liable for the infringing activities that took place within the network. This could lead to the shutdown of a node either due to a judicial order or due to the fact that the owner does not feel like carrying on the activity anymore. In either cases, if this person owns a critical node, the shutdown of the node could hinder the functioning of the entire CN.

[9] 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>).

[10] 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).

Given these premises, the choice of a CN on whether or not to organise itself as an association and the way this choice is put into practice gain a lot of importance. We already said that an effective distribution of the network can make the network stronger: this is true also in terms of distribution of legal powers.

5 Conclusions and Future Works

In recent years there has been an increasing interest in alternative media that can help people re-acquire at least some control over personal communications. Most of the efforts has been focused on software platforms that guarantee anonymity and resistance to censorship but CN provide an excellent example of bottom-up initiatives that try to subvert the physical architecture of the Internet itself, which is at the base of its fragility. CNs are indeed a variegate world, they diverge from country to country, from community to community but many of them share the goal of building new, bottom-up communication infrastructure managed by the people, and not by some untrusted third party. This is a daunting task since the structural fragilities of a network are hidden in many different aspects, technological, social and also legal.

In this paper we studied the case Ninux.org, the largest Italian CN and one of the first to be created in Europe. Our goal was to identify the motivations and goals that drive the members of the community and relate these motivations and goals to a set of measures that can be verified on the infrastructure of the network, with the added complexity of considering also legal constraints to these networks, another key dimension to reflect on CN's sustainability and opportunities.

Our analysis shows that Ninux roots its action in values such as the freedom to communicate and the decentralization of the infrastructure as an alternative to the commercial and political exploitation that corporations and governments do of communication media. Decentralization and distribution seem to be the keywords that make Ninux intrinsically different, and that should guarantee its development as an "alternative Internet". Instead, the technical analysis we performed shows that the sole fact of being "distributed" does not guarantee that a CN is effectively different from a hierarchical, traditional network. We have shown that the mobilization of activists and participants, together with the intrinsic difficulties related to the bottom-up construction of a network, does not generate an effectively decentralized infrastructure in the Ninux topology; on the contrary, the network evolves with inconsistencies that are not introduced "by design" as in traditional networks, but emerge from the process spontaneously. These points of failure are concentrated in a few network nodes, in a few people that own them, and in a few people that lead the discussion in the mailing lists. Under a legal point of view the concentration of responsibilities (even if only informally existing, and not explicitly assigned) makes the network weaker. Even if the network has no legal representative, it has a small set of people and nodes that could be the target of legal actions aimed to fracture the community and discourage its growth.

CNs need to develop their own instruments to monitor their evolution and verify that the implementation of the network represents a satisfying compromise between the goals that the community sets for itself and a manageable network infrastructure. Even if we can not give here the solution, we can suggest guidelines to improve in the future, based on the enrichment of the technological instruments that Ninux uses (and other networks too). A direction of improvement is to modify the mapserver we described in sect. 3 to show the following information: the centrality of nodes, which can be visually embedded in the map changing the size for the nodes in order to reflect their centrality, and the ownership of nodes, which can be displayed with different colors. Since the mapserver is a key element in the management of the community, even introducing these simple features would put at the attention of the community the predominance of some nodes and members of the community. This would in turn help to find solutions, such as the creation of nodes that subtract some importance to 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 to periodically take the 'pulse' of the community with a survey about the network features which can be submitted to each member in the community. The survey would first disclose information about the network itself (growth of the network, of the community etc.) in order to interest people and would ask questions about such

features, for instance, about the perception that the user has on the distribution of the ownership of nodes or the number of critical nodes. Similarly, the legal perspective can enter the evaluation with questions about the predominance of the use of a certain Internet gateway on the others. From the answers to the questions, the community will set the thresholds that express the level of satisfaction to the way the network is evolving, and provide the input to initiate the discussion among the community participants about how to solve the issues that eventually emerge.

Finally, we want to stress the importance multi-disciplinarity had in our work. A socio-technical experiment like a CN can be hardly studied under the light of a single discipline, since the importance of these networks resides in their multi-faceted nature. This paper developed a multi-perspective framework from the very beginning, and this output only represents an initial effort of a joint work that will continue in the future in order to propose and put into practice deeper understandings and actual solutions to the problems we posed, with the final aim to help the development of more democratic and more open community networks.

Bibliography

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

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

Atton, C. (2001) *Alternative media*, London, Sage.

Baig, R., Roca, R., Navarro, L. & Freitag, F., (2015) Guifi.Net: A Network Infrastructure Commons. *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development, ICTD '15*. ACM, New York, NY, 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). p. 111-130.

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

Bird, C., Gourley, A., Devanbu, P., Gertz, M. & Swaminathan, A., (2006) Mining Email Social Networks. *Proceedings of the 2006 International Workshop on Mining Software Repositories*, MSR '06.

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

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

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

Carroll, J.M. & Rosson, M.B. (2008) Theorizing mobility in community networks. *International Journal of Human-Computer Studies.* 66. p. 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). p. 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. & Treguer, F. (2015) Expanding the Internet Commons: The Subversive Potential of Wireless Community Networks. *Journal of Peer Production.* 6. p. 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, p. 1-9.

Frangoudis, P.A., Polyzos, G.C., & Kemerlis, V.P. (2011) Wireless community networks: an alternative approach for nomadic broadband network access. *IEEE Communications Magazine* 49, p. 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). p. 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. p. 957-979.

Giovanella, F. (2015) Liability issues in Wireless Community Networks. *Journal of European Tort Law.* 6 (1). p. 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. & Margolis, S.E. (1994) Network Externality: An Uncommon Tragedy. *Journal of Economic Perspectives.* 8 (2). p. 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). p. 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. & Lo Cigno, R, (2015) A week in the life of three large wireless community networks. *Ad Hoc Networks.* 24.

Maccari, L. Baldesi, L., Lo Cigno, R., Forcono, J. & Caiazza, A. (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 Ayers ,M. D. (eds.) (2004) *Cyberactivism: Online Activism in Theory and Practice*, Routledge, New York.

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). p. 1435-1448.

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

Page, W.H. and Lopatka, J.E. (2000) "Network Externalities", in Bouckaert B. and DeGeest, G. (eds.) *Encyclopedia of Law and Economics*, *Volume I. The History and Methodology of Law and Economics*, Edward Elgar, Cheltenham, 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*, Roma, Derive Approdi.

Pelizzoni, L. and Ylonen, M. (2012) *Neoliberalism and Technoscience: Critical Assessments*. Ashgat, United Kingdom.

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

Robert, R., Manulis, M. De Villenfagne, F. et al. (2008) WiFi Roaming: Legal Implications and Security Constraints. *International Journal of Law and Information Technology.* 16 (3). p. 205-241.

Schuler, D. (1994) Community networks: building a new participatory medium. *Communications of the ACM.* 37 (1). p. 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). pp. 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). p. 423-450.

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

Verbiest, T., Spindler, G., Riccio, G.M. & Van der Perre, A. (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 June 20, 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.