Forced to live side by side

Power, privacy and conflict in the Tor network

A thesis submitted for the degree of

Doctor of Philosophy

BY

Daniele Pizio

School of Business

University of Leicester

March 2021

Forced to live side by side. Power, privacy and conflict in the Tor network

Daniele Pizio

Abstract

The Tor anonymous network (acronym of *The Onion Routing*) is a socio-technical object of extraordinary complexity the significance of which cannot be reduced to the trivial "Dark Web" media narrative usually employed to depict it. Originally conceived as a technical fix to mitigate the design flaws that affect the Internet architecture and have made electronic mass surveillance possible, Tor has progressively evolved into a distributed open source network which nowadays sees the participation of thousands of activists, academics, diplomats, army engineers and ICT company technologists. Its development trajectory has been influenced by numerous hacker cultures that have found in the infrastructure a space of cohabitation and experimentation suitable to fine tune new technological prototypes and political practices. These have been elaborated and tested in multiple historical contexts, such as the so called Arab Spring, the Anonymous movement, the Snowden's leaks, the rise of whistleblowing platforms in journalism, as well as the US State Department's digital diplomacy and the efforts made by Washington and Silicon Valley to secure the US digital infrastructures.

The thesis analyses the material configuration of the Tor infrastructure whose technical features and organizational practices contributed to the emergence of these different involvements with Tor. In order to achieve this objective, the study a) traces a genealogy of the imaginaries embodied into Tor and the power relationships that model its infrastructure and functions, b) investigates how its developers interpret the concept of privacy and incorporate it into the platform, c) explores the politics and practices adopted by the Tor community to ensure the sustainability and the usability of the network. The research design of the study is a three-year long ethnography of the infrastructure. The analysis of Tor is structured around a careful reading of its fundamental design papers, an examination of the financial statements made public since 2008 by the Tor Project and a collection of interviews featuring twenty people who contributed at various levels to the growth and the maintenance of the network.

From this work it emerges that Tor is an experimentation platform crossed by subjectivities often different to one another but still forced to live side by side in order to engender practices and technologies that disrupt the power relations constituting the contemporary Internet and generate alternative ways of existence. The thesis contributes to the field of Science and Technology Studies concerned with Internet governance, as well as the organizational forms adopted by social movements within the current age of surveillance capitalism.

Acknowledgments

I wrote a big part of this thesis in Bergamo, while the COVID-19 epidemic was at its height and thousands of people all around me were dying. As much as watching an entire generation of people disappearing in a few days has been tremendously painful, I believe that it is absolutely crucial to treasure that pain in order to urgently question and challenge the neo-liberal infrastructures around which the lives of billions of people are organized. In those dark days, I was forced to live side by side with my mother Nuccia and my brother Marco with whom I was able to create a fragile equilibrium of coexistence and to elaborate many forms of mutual support and aid: thanks for your efforts and the love you show me. Another thanks goes to Martina who, for reasons which are not yet entirely clear to me, keep loving and supporting me with patience and enthusiasm, always showing me with sweetness and acumen my limits and helping me to overcome them. I hope one day to be able to give you back even just a little of what you have been able to give me over the years. Thanks to my supervisors: Amanda Earley and, particularly, Dimitris Papadopolous, who has often tolerated my dumb arrogance and has patiently kept pushing me to reflect on the complexity of technologies I thought to know. Shout out to my fams in Leicester who, when the PhD was looking endless and meaningless, have been of extraordinary support: Margherita, Marco, Maddalena, Matteo, Milena, Paul, Blanka, Chiara, Andrea, Martina, Nerina, Vivian, Marisol, Changyo, Terrence, Ilaria and Stefano.

Thanks to the people, in Italy and all over the world, who keep fighting and crafting technologies for distributing power and creating many possible futures: the Tor Project and all the people who have spent their time for helping me with this research. Along with them I cannot forget to mention Tails, void, McSilvan, SignorK, Autistici/Inventati, Riseup!, Anonymous, Qubes, claudio, obaz, putro, shammash, szara, Raffa, Jigen, Eddi, Jacopo, YPG/YPJ, Carola, Mascio, Pierpaolo, pakcz, Lorina, Gianluca, Betta, Martin, Katja, Karlessi and Hanay. Another thanks goes to Benedetto Vecchi whose words and writings have always been enlightening and stimulating: we really miss you comrade. I cannot forget professor Maurizio Ricciardi and professor Sandro Mezzadra, without whom this journey would have probably never started. Props to Gianpiero, Josip, Aleajandro, Duvan, Luis, Hans, Robin, Mario, Mattia, Martino, Timmy, Pierluigi, José, Rafael and all those who brought me one step away from stars.

This thesis is dedicated to the memory my father Gabriele, my cousin Gomati and my aunt Mirella, who passed away while I was writing it. I miss them every day.

Table of Contents

Chapter 2. Methodological approach to infrastructure

Chapter 3. The Tor's funding system

Chapter 4. Privacies

Chapter 5. Tor politics

6. Conclusions

Appendix A: ethics-by-infrastructure

List of figures

List of Acronyms

ADSL: Asymmetric digital subscriber line

BBG: Broadcasting Board of Governors

BBS: Bulletin Board System

C4ISR: Navy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CA: Certificate authority

CHACS: Center for High Assurance Computer Systems

CISE: Computer and Information Science and Engineering award

DARPA: Defense Advanced Research Project Agency

DNS: Domain Name System

DoD: US Department of Defense

DoT: Dns-Over-Tls

DoS: UD Department of State

DRL: UD Department of Rights and Labour

EFF: Electronic Frontier Foundation, an US historical civil rights association

FH: Free Haven

FLOSS: Free and Libre Open Source Software

FTN: Fault Tolerant Network

GAFAM: Google, Amazon, Facebook, Apple, Microsoft

GIFT: Global Internet Task Force

GP: Guardian Project

GSA: US General Service Administrator

IBB: International Broadcasting Bureau

ICANN: Internet Corporation for Assigned Names and Numbers

ICT: Information Communication Technology

IETF: Internet Engineering Task Force

IN: Internews Network

IoT: Internet of things

IP: Internet Protocol

IPDRL: International Program to Support Democracy, Human Rights and Labor

ISOC: Internet Society Conference

ISP: Internet Service Provider

LFP: Library Freedom Project

NFTF: Net Freedom Task Force

NRL: US Naval Research Laboratory

NSA: US National Security Agency

NSF: US National Science Foundation

ONR: US Office for Naval Research

OONI: Open Observatory of Network Interference

OTF: Open Tech Fund

OR: Onion Routing

OS: Operative Systems

OSINT: Open Source Intelligence

OWS: Open Whisper Systems

P2P: Peer to peer

PDA: Personal Digital Assistants

PET: Privacy Enhancing Technology

PT: Pluggable transport

RFA: Radio Free Asia

RFC: Request for comment

SIDA: Swedish International Development Cooperation Agency

T/A: Traffic analysis

Tails: The Amnesic Incognito Live System

TBB: Tor Browser Bundle

TLS: Transport Layer Security

Tor: The Onion Routing

TPI: Tor Project Inc

UI: User Interface

UX: User Experience

VPN: Virtual Private Network

Introduction

During my first PhD year – while I was struggling to keep up among the compulsory training modules, the impostor syndrome, the pressures of my supervisors for finishing as soon as possible the literature review concerning the concept of infrastructure – I stumbled (I do not remember how) upon a paper written by a German researcher who I had never heard before. The topic of the essay (Höne 2015) – one among of the many that I haphazardly printed in a desperate attempt to elaborate a theoretical framework for the upcoming supervision meeting – was the inauguration of the New York metro occurred on October 27, 1904. Particularly, the author focused his attention on the emotional reaction unleashed by that event among the citizens of the Big Apple. Although the topic was apparently little relevant to the subject matter of my research, I started to avidly read it, mostly being enticed by the lively and ironic style of the author.

Yet, line by line, a topic started to make its way among the themes discussed in the essay; a pivotal one, that yet I had not been able to trace in the literature I consulted until then, that is the relation that inevitably arises among infrastructures, imaginary and future. As I discovered, by reading with growing interest, the opening of the first underground transport line in NYC was reason of great hope and excitement among the city dwellers, so much as to powerfully make its way in the collective imaginary, by cutting through, even if for a single day, the boundaries of the ethnic and class divisions which already made up the geography of the metropolis at that time. The subway *grand opening* had been prepared for a long time by the city authorities. For the occasion, these latter elaborated a discursive regime aimed at lessening the possible concerns of the future passengers with regard to the security of the new underground infrastructure. In order to achieve this goal, city elites, the political class, local media, social reformers and businessmen embarked in an operation of radical redefinition of the 'underground' imaginary, by hailing the advent of the new mean of transport as a moment of renewed prosperity and social reconciliation. Furthermore, they publicly associated the new forms of mobility made possible by the tube with promises of economic growth and of a better future.

But what really struck me about Höne’s paper was the account of the frantic, almost hysterical, reactions by the New York citizens on the inaugural day of the line. The great deal of expectations fanned in the previous months, along with the new sensorial experience of an underground high-speed travel, caused a giant wave of euphoria that got out of the authorities' control and overwhelmed hundreds of thousands of people. When the opening day came, thousands of onlookers crowded all around the station where the train was supposed to arrive after the inaugural tour. As soon as they saw that clanking marvel made of glass and steel popping up from an underground gallery, they burst into jubilant shouts and amazed remarks. Somebody started to ignite fireworks in the sky in order to express her enthusiasm, while the sirens of the boats sailing on the Hudson river rang all around. In no time the metro stations were flooded with people who queued for hours in order to buy a ticket and experience that new exciting adventure. Many of them ran in circles on the wagons for hours, crossing neighborhoods they perfectly knew or where they would have not set foot again for the rest of their lives. The novelty of that experience was so unsettling to trigger unexpected, unadvised and uncontrollable reactions among those who were living it.

It is a sensation that I perfectly understand and that I have felt most of the times I encountered a new technology during my life. I can definitely say that I feel a sense of familiarity with the chaotic euphoria that characterized that carnivalesque New yorker afternoon of over a hundred years ago. In that uncontrolled enthusiasm I saw many of the hopes – and the naivety as well – that marked my relation with Tor through the years. I clearly remember when, during a night of September 2005, I discovered this low-latency anonymity network for the first time. I had already heard a lot about it in the circles I was used to attend, most of them being linked to the local social movements in Bologna (the town where I lived at that time). Anyone was talking about it enthusiastically, presenting it as a tool that would have frustrated any attempt by the police to track our online movements. Thus one evening, when I was at some friends' place, I decided to take advantage of their excellent ADSL connection – a rarity at that time – in order to deepen my knowledge about the topic. After everybody went to bed, I grabbed an Ethernet cable dangling from the desk where the router was placed and plugged it into the RJ45 port of my laptop. Then I downloaded from the Tor Project website the software to connect to the network and, once configured, I launched it from my computer. I waited for some minutes – at that time the speed of Tor was ludicrous, also because of the limited number of relays its infrastructure was made of – until a message appeared on the monitor: *"You are connected to the Tor network*". Boom! Although at the time I was still using Windows XP, even the simple fact of having correctly configured a proxy made me feel like a black-hat hacker. I clicked on the Mozilla logo and entered the URL http://www.whatismyip.com in the navigation bar. The loading of the website was awfully slow, but the feverish excitement I felt under my skin suggested me to not desist and keep the browser window opened. After almost 5 minutes of waiting, a US IP address appeared before my eyes, accompanied by the icon of a star-spangled banner featuring at its bottom these words "Location: San Francisco". I was left agape, astonished. I closed the browser, opened a new circuit towards the Tor network and entered the same URL again. This time I was in France. Then in Germany. Then in the US again. I spent the following night hours to repeat the same actions, hopping like an idiot from an IP address to another, absolutely shocked by the possibility of assuming whatever identity I wanted and being in two continents at the same time. That night was my carnival. I started to generate encrypted traffic towards most trivial news websites that I read daily. Then, I moved to something different and I reconfigured every possible program (even some I had never used) so that their traffic would be routed through the Tor network. Ultimately, I tried to read the Tor manual (truth to be said, without understanding much of it), until when, at the crack of dawn I collapsed, exhausted, on the sofa next to the computer. On the next evening I showed up at the weekly assembly of my collective with two big dark circles under the eyes, confusedly praising the magnificent advances of that tool, attempting to explain the use we could make of it. In response I received puzzled looks, ironic chuckles and patronizing pats on the back. Pretty embarrassing, but I did not care about that. I thought it was done. Thanks to Tor the Internet was going to become a territory out of the control of cops and multinationals, where we could have become unstoppable and we could have self-organized in order to give life to that cherished revolution we dreamt of so much.

To be honest, it was not the first time it happened to me to go nuts in front of a new technology. Just a couple of years before a comrade made me discover Napster and my reaction was more or less the same: "It is done! Intellectual property is on its way out: this is the swan song of capitalism!". Blessed youth who sees what is not there, but you have to understand it. After all, as Musiani (2012) wrote, the charm of peer-to-peer (P2P) technologies is to be found not only in the technical efficiency characterizing them, but also in the strong feelings that such networks are able to evoke. The lack of centralization in their design, the few resources being necessary in order to use them and the process of active cooperation that involves a multitude of users seem a reference to the Internet original culture and to its democratic imaginary of decentralization and distribution of power. In this perspective, Musiani also emphasized how P2P network infrastructures (and in my opinion this reasoning applies to Tor as well) were intended for a long time as a form of politics and, probably, also envisaged as a substitute to it.

Today for me Tor has become a tantamount of what the metro of New York represents for its dwellers. This network has sunk into my daily life and the objects through which I lead it. It is rare for me to surf the web – it makes no difference whether on a laptop or a mobile phone – without using Tor Browser. Also, Onion services (untraceable and geographically hidden web services hosted in the Tor network) became a must in my daily organization: I use them for chatting, for sending mail, for administering my router and other objects connected to the Internet, as well as for performing updates on my computer. Moreover, my research data and notes – except for the most sensible ones that never saw the light of a public IP address – are entirely stored on an onion server which I physically control and administer. But these are only a few uses among those I make of the Tor network (to which I contribute myself by running a certain number of relays). I am surely forgetting most of them. The fact is, they have basically become invisible. For me, simply, Tor does exist, it works and it is perfectly tailored to my daily routine.

It has also to be said that the degree of power that I have at my disposal when I use Tor has become more and more clear to me over the years. My ISP cannot associate my identity with the online activities I normally carry out. It does not know which websites I visit, nor my position when I connect to my home network from outside and not even which services I am using. Tor anti-tracking features give me some additional chance of not being targeted by advertisement campaigns or unwanted spam. My email provider cannot trace back my IP address, not even if it wanted to. Moreover, each time I need to create a secure access to a network I quickly setup an onion service without the need of relying on any commercial company: I do not need a static IP address anymore, nor a dynamic DNS, nor to buy an encryption certificate to protect the confidentiality of my connections, and not even to rent a virtual private server, a second level domain or a premium service to mitigate possible DDOS attacks. All of these properties are already deployed by default in Tor onion services.

Yet, it is now clear that these technical properties (and the power resulting from them) are neither of exclusive interest of nerds like me, nor of groups of ethical hackers (like the Northern American Riseup!, the Italian Autistici/Inventati or the German Systemlii) interested in ensuring to users a communication as much free as possible in this age of liquid surveillance. Nowadays among the admirers of Tor there are also those same corporations and cops that I thought would have considered it as an enemy to relentlessly counter. Truth of the matter is different. The most important onion service on the web today is Facebook. Beside Zuckerberg's social network, the number of Silicon Valley companies who are investing time and resources in developing Tor is increasing: among the most important we can count Mozilla and Cloudflare, along with a myriad of smaller firms. And State institutions are very present on the Tor network as well: for instance one can find the CIA – who uses its onion service to recruit potential snitches and to hire new staff office –, while the US Department of Defense and Department of State have been its main funders (even though for different reasons). And this not to mention the global and local media mainstream outlets resorting to Tor in order to implement whistleblowing platforms or to grant uncensored access to their websites: they are countless.

The heterogeneity characterizing Tor is a direct consequence of its technical properties and their capability to produce a reconfiguration of power and authority online which is compatible with an agglomerate of political visions, often very different to one another. In this thesis I aim to unveil the plurality of imaginaries embodied into the Tor infrastructure and the role this latter plays in a historical context where the Internet has become fully undemocratic and surveilled by default. For this reason, I will also investigate how the Tor developers interpret the concept of privacy and translate it into the technologies they create.

1. Approaching Tor through history and theory

1.1. Governance

Nowadays the Internet is a vast and complex ecosystem being managed through numerous governance practices, that is to say, mechanisms of political organization being characterized by a multicentric rationale and being operated by a plurality of actors. In fact, its governmental functions are ascribed to a network of institutions, agencies and companies who are endowed with the legitimacy of autonomously activate and exert them, albeit in an operational context of mutual coordination. At the same time, the dissemination of the Internet on a global scale has made it more complex for nation-states to exert their sovereign authority within their jurisdiction. As argued by DeNardis and Musiani (2016, 4), Internet governance “transcends traditional government-centric mechanisms" and it is being “collectively enacted by the design of the technology, the policies of private companies, and the administrative functions of new global institutions like the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF), as well as national laws and international agreements”. Governments, business corporations, standard-setting bodies, traditional political institutions, bureaucracies and NGOs compete in order to put their hands on the “hidden levers of Internet control” (DeNardis 2012, 720). This expression refers to tools such as technical standards, protocols, infrastructural design choices, web regulation laws, private policies, terms of service and trade agreements that, according to the scholar, have arisen to a two-pronged role through the years. On the one hand, they define and guarantee the minimum level of operability and efficiency of the Internet. On the other hand though, they can be easily co-opted in order to carry out goals different than those they were originally conceived for (a dynamic common to many other technologies, see Tenner 1997) and that have nothing to do with network infrastructure administration in the strict sense.

Actually, the hidden levers of Internet control proved to be excellent "proxies to regain (or gain) control or manipulate the flow of money, information and the marketplace of ideas" (DeNardis and Musiani 2016, 4). Moreover, they embed political choices and cultural attitudes, namely "a given mindset [that] gets externalized and unloaded onto a tool, where it no longer needs of thought to activate itself" (Bridle 2019, 22). Taking control of such levers means having the power to give the Internet the shape that is most deemed suitable for the pursuit of one's values, interests and purposes. Hence, the Internet infrastructure is not limited to the stand-alone presence of the subjects partaking in its governance, nor to the power resulting from the technical functionalities that they are called to separately fulfill. On the contrary, it is actually given at the “infra” level – that is, "in the relation between subjects interacting in a space that is not a territory, but a framework of reciprocal exposition being generated by [their] co-presence" (Sparti 2015, 162). In other words, at the heart of Internet governance there is the relation among the actors who control important Internet technical functions and, by using the resources at their disposal, create dynamics of reciprocal influence with the goal of "reorganize institutions, legitimize knowledge, produce structures of authority and political geographies [...] and give birth to new power (im-)balances” (DeNardis and Musiani 2016, 9). Therefore, as any other technology the Internet has politics, meaning that it incorporates and reproduces “arrangements of power and authority” (Winner 1986, 22) that, nowadays, seem to be expression and vehicle of a radical imbalance in the distribution of opportunities, privileges and justice.

Indeed, out of the thousands of players who partake in its governance, only a handful is able to direct the ends for which the Internet is built and the modalities (such as, technological standards, laws and political economies) through which they shall be reach. The very topography of the Internet is the plastic representation of this concentration of power and it has made obsolete the metaphor through which the web had been conceived for long time – that is, the one of the rhizomatic “network of networks". The rhizome, as Umberto Eco recalled (2019, 689-90), "is made so that each road can connect with any other. It has no center, it has no periphery, it has no exit, because it is potentially infinite". Quite the opposite of what the Internet has become today, namely a platform being structured into a limited number of macro regions, technological clusters and private digital networks belonging to a few US companies, where enormous amount of data are stored and centralized (Musiani 2012, 3). According to the KRITIK collective, the network has become a territory "increasingly broken up, modular, vertical, stratified" and organized "in media that we could define as clusters" (2019, 17). As noted by Sordi and Fioramonte (2019, 24), the contemporary web looks like 1965 Beijing's tube, that is “two lines from (and to) which all the nodes of the network converge”. Indeed, similarly to what happens to the traditional media sector, today the web is affected by two intertwined tendencies: a maximization of the number of users that, in turn, is matched by the presence of a relatively low number of transmission sources (Milani and Sasso 2015, 5).

The origin of this topological gigantism dates back to the first half of the '90s. In 1992 the project of privatization of the web kicked off: private capital injections progressively started to flood the sector, alongside public financing allocated by US political institutions (which, until that moment, had been the main funding source to support computer science research, Castells 2002, 40). Precisely while the Internet was becoming a mass medium – either because of the rapid diffusion of digital devices and the simultaneous fall in data storage and hardware costs –, it was reconfigured with the goal of turning it into an environment compliant with the needs of venture capitalism. According to Kleiner and Wyrick (2007), this transformation occurred following two different paths. First, the peer-to-peer (P2P) model [1] – which utile then had characterized the development of the web – was sidelined and replaced with the hierarchical client-server one. Concurrently, home broadband ADSL connections (acronym of ‘Asymmetric digital subscriber line’) started to spread, providing customers with high download capacity at the expense of their upload capacity. Client-server model and asymmetric connections favored an increased end-users reliance on commercial external services, thus enabling a widespread process of control, acquisition, analysis and exploitation of their personal data for economic purposes.

In the medium term, these design choices, alongside with a political process of market deregulation that started in the first half of the '80s, favored the occurrence of an unprecedented oligopolistic concentration in the history of capitalism (Formenti 2011, 130), which matches the aforementioned topological gigantism characterizing the current shape of the Internet. As a matter of fact, in the Information Communication Technology (ICT) sector, the companies that first reached and then strengthened a dominant position can be actually counted on one hand: they are the so-called information intermediaries, also known as over-the-top (OTT). We are talking about global corporations whose role is essentially that of being a *liaison*, to build a bridge over the ocean of information separating a user from a content being published on-line, thus facilitating the access to it. Google, Amazon, Facebook, Apple and Microsoft – often being referred altogether under the GAFAM acronym – are the most prominent data brokers on the market. According to a report published in 2014, four of these companies (Microsoft was not included in the analysis) had a projection of growth that in 2020 would have led them to become the first economic power on the planet (Fabernovel 2014).

Although they are often perceived as aseptic channels of communication, Californian Internet companies' platforms have been actually conceived and implemented according to two design criteria. The first one is *universality*. Technological firms work to unify and stratify an ever-increasing number of functions within a single device with the aim of creating, not just a tool, but *the* universal tool: an object suitable for fulfilling any purpose, satisfying any desire, a true meta-infrastructure on which should depend the functioning of any other infrastructure around which life is organized (KRITIK 2019, 22). The second one is *surveillance-by-default*. Indeed, commercial social media, search engines and instant messaging platforms are environments aimed at surreptitiously inducing users to produce personal information that is constantly monitored, aggregated and sold to the highest bidder (Lovink 2008; Ippolita 2014). In the so-called "Web 2.0", participation to social communication processes entails an implicit submission to widespread surveillance mechanisms (already in progress in the age preceding the advent of social media, see Lyon 1997 and Rodotà 2004) being geared towards an intensive exploitation of users. Furthermore, such platforms are devices for normalizing diversity. Being kept under constant control and profiled by invisible algorithms, within these environments users are targeted with information and contents that reflects their preconceived opinions: that is, they are confined in homophilic bubbles in which their symbolic and perceptive structures are manipulated without them realizing it (Parisier 2012). Nowadays this dynamic is intensified as the owners of these private digital environments are also the main players in the emerging sector of the Internet of Things (IoT), being characterized by products such as wearables, nearables, drones, smart cars, smart TVs and domotics. These neologisms, that have suddenly entered the everyday vocabulary, hide behind their semantic nebulousness the transformation of items of everyday use into computers being purposely programmed in order to generate a constant flow of personal information.

Ubiquitous, invisible yet deeply material, embodied into daily routines and social communication processes, automatically triggered by miniaturized technologies implemented on a mass scale: this is the current state of surveillance that, after having been perfected for more than a century as a governmental technique (Bowker and Star 1994), has gone beyond the scope of state sovereignty and has became the crucial element of "a new logic of accumulation [that] quickly spread from Silicon Valley to every economic sector" (Zuboff 2019b, 11). Governmentality through surveillance ceases to be a sole competence of politics: indeed, when operated by corporations, its goal is not anymore to achieve "a long-term, stable and docile society" or to strive "for the optimal use of resources to reach government-issued goals" but rather to set short-term objectives in order "to control specific parts of – increasingly international – markets" (Galič et al 2017, 19). In other words, contemporary surveillance practices, instead of disciplining and punishing, aim to organize a population on a globally scattered territory with the goal of maximizing its economic potential (Cacciari and Pizio 2015).

Pursuant to these transformations, information intermediaries have been vested with an extraordinary power. Indeed, besides the crucial role they play in the social communication practices (Vecchi 2015) and the above mentioned dynamics of topographic gigantism, infrastructural centralization, economic oligopoly, a creeping privatization of the public sphere has to be mentioned as well. According to several authors (DeNardis 2010; Papacharrisi 2010; Vaidhyanathan 2012), GAFAM's ability to control some fundamental technical levers of the Internet has put them in the position to privately exert several functions once being considered as public. The phenomenon, which sees nation-states delegating some of their governmental functions to private corporations, goes far beyond the field of Internet governance: indeed, it involves several bureaucratic institutions and must be regarded as "part of broader political conditions" (DeNardis 2014, 13). As stated by Sassen (2008, 74) "since public regulative and legislative functions become more and more subordinated to technical standards that make possible the globalization of corporations, we can witness the emergence of a substantially private agenda within the framework of a formally legitimated public authority". To say it in another way, technical standards being issued and enforced by private players have taken on a public regulatory function.

In fact, nowadays GAFAMs, besides being information intermediaries, also became privacy protection gatekeepers. As owners of private infrastructures, they are the only actors entitled to give access to users data when they are asked by a government. Yet, this power has been arbitrarily exercised, as it "has benefited some governments more than others" (Sargsyan 2016, 189). Indeed, the revelations of former NSA contractor Edward Snowden provided a material evidence of how the major Silicon Valley corporations have been active upholders of Washington's interests, by signing backroom deals according to which they lent their technological and commercial infrastructure to US power politics (Greenwald 2014; Snowden 2019). Big Tech companies have granted to several federal intelligence and law enforcement agencies an exclusive and preferential access to users' data that, when adequately processed, can turn into formidable tools of espionage and levers of political and economic influence. In exchange, US OTT companies obtained a soft legal framework and the possibility of resorting to technological and juridical self-regulation practices. "The phenomenon", Sargsyan argued (2016, 193), on the one hand "results in granting the companies an uninformed consent to operate based on their commercial interests", while on the other "marks the limitation of national laws and the dependence of nation-states on private companies' infrastructure and decision making".

This latter consideration needs further clarification, without which the role of the state in the Internet governance processes would risk to be excessively overshadowed. It is beyond any doubt that through the years the current Internet configuration, and the distribution it has produced, elicited a growing frustration in the governments all over the world. China, Russia and Europe are increasingly inclined to identify in the Silicon Valley a vector of US cultural, political and financial hegemony (Formenti 2012). As a matter of fact, in the last two decades the Internet has been the object of several bipartisan initiatives undertaken by Washington political institutions in order to achieve two goals: first, to make it compliant with particular North American liberal values – that is "a non regulatory, market-oriented approach to electronic commerce" and "an anti-censorship principle […] originated as a component of the effort to promote electronic commerce" (Goldsmith 2018, 4); second, to transform it in a robust global commercial platform and to "export to other countries US notions of free expression and free trade" (ibidem). Furthermore, GAFAM's current privileged position in the global market is not only due to the creative genius of a generation of visionary entrepreneurs (often symbolized by the iconographic figure of Steve Jobs). On the contrary, their power mostly originated from the wise vision of an "entrepreneurial state" that with its policies made possible a vigorous growth of the Californian industry. Originally being explored by Castells (2001, 33) – who explained how "all the crucial technological developments which led to the development of the Internet found their breeding ground within governmental authority, big universities and research centers" funded with public money –, this concept has been lately formalized by Mazzucato (2018). According to the scholar, after the WWII the US state has developed a proactive industrial politics aimed at shaping the market, encouraging innovation and boosting the technical progress. It did so by using all the tools at its disposal, such as "public procurement […] contracts and regulation" (ibidem, 103-4) and by taking risks that the private sector would have never taken in the long term. Mazzucato claims that "the miracle of Silicon Valley […] is the result of huge investments that, even if decentralized, have been led by the public sector" (ibidem, XXII). Indeed, between the '80s and the '90s, Washington promoted most advantageous fiscal policies for the emerging Internet sector. For decades, it also funded the development of basic and applied scientific research, which innovations were first employed in the military field and then, converted to civil use and commercialized. Hence, if it is true that, as Sargsyan claims, many nation states have developed a strong dependence on foreign private infrastructures, it is also true that such dependence is the result of specific Washington policies, aimed at stimulating the growth of its own national champions in order to turn them into a tool of global conquest. It is not by chance that several US centers of power – first and foremost the State department – for a long time have conceived the cyberspace as a disruption network for interfering in the sovereign policies of state bodies being considered as hostile, by resorting to practices of media propaganda dating back to the cold war (Morozov 2011, 33-54; Powers and Jablonski 2015, 27-49).

Yet, this inextricable bond between Washington and the Silicon Valley is also one of the driving forces that is contributing to redesign the Internet political geography. Indeed, the power imbalances resulting from it have led many states to undertake various initiatives with the goal of taking back sovereignty over their own digital spheres of influence. By resorting to different strategies, Germany[2], Russia[3], Turkey[4] and China[5] are establishing geo-technical boundaries around their national spaces. In particular, Beijing and Moscow are banning the use of foreign software and, where possible, they urge local authorities to replace it with local products. Brazil[6] has tried to build new undersea cables directly connecting the country with Europe in order to avoid data routing towards US data-centers. China has signed agreements with Apple[7] and has provided it with access to its internal market as long as it agreed to locate its data servers on Bejiing national territory. Bruxelles has repeatedly fined several US companies for violating local regulations about privacy, competition and intellectual property. In other words, a real Internet balkanization (Goldsmith and Wu 2006, 51-127; Formenti 2008, 208) is going on: digital networks are progressively acquiring the features of the local context where they unfold – that is, they are colonized with particular territorial values (Saco 1999) – and more and more autarchic networks rise, being closely monitored by police and local security agencies (Lovink 2012, 27-30). Silicon Valley surveillance has engendered even more surveillance in response to it.

1.2. Power

How is the Internet infrastructure transforming the status of its users? How does it change our experience of the world when we live under surveillance 24 hours per day? What are the needs legitimizing the existence of a network with such features? What are the social values being legitimized by its presence? What are those being disqualified instead? Ultimately, what are the social structures resulting from them and the power relations between rulers and ruled that they underlie?

Bruce Schneier (2015) defines the condition experienced by Internet users as an unfair bargain. Internet companies provide free services in exchange for surveillance which "enables discrimination based on almost any criteria: race, religion, class, political beliefs", and it is used "to control what we see, what we can do and, ultimately, what we say" without offering citizens "any real ability to opt out, and without any meaningful checks and balances" (ibidem, 4-5). La Cecla (2015) argues instead that the removal of secrecy from social rituals undermines the processes of creation of identity (which are operated through mechanisms of inclusion and exclusion that define the perimeter of the group membership), as well as its renewal (without secrecy the individual is stuck to a past she cannot escape from). According to Boyd and Crawford (2012), the Internet is an expression of a new "digital divide": resources are unfairly distributed and only a few individuals can access the data being produced by the mass of users. Richterick (2018) affirms that this asymmetry in access to resources mirrors the asymmetry of power characterizing the structure of our society: data monopolies symbolize the opposition between elites and masses and they are reason of social injustice.

Similarly, Zygmunt Bauman and David Lyon (2014) claim that "liquid surveillance" is the praxis upon which the power has based a new social contract: this latter entails the decay of the status of "citizen", its replacement with that of "commodity" and the end of any negotiations between rulers and ruled. According to the two authors, the new forms of digital surveillance are to be deemed as liquid because they affect any scope of social life whilst aiming at dissolving any form of bond structuring it. Its function is the one being historically ascribed to traditional surveillance – that is, "to preserve hierarchy and class distinctions" and "to distribute possibilities of life, opportunities, rewards and privileges” (ibidem, XXIII) – but the extension of its reach produces an asymmetry of power “without any possibility of reciprocity” (ibidem, XXII). Indeed, the individual experiences a condition of absolute transparency in front of surveillance, while the organizations monitoring her can enjoy an utter opaqueness. These latter manage a technical apparatus that is incomprehensible (due to its technical sophistication), ubiquitous (because it is embedded in daily use infrastructures) and secret (because of its importance for national security and competition between private companies). Moreover, its pervasiveness entails the erosion of individual autonomy and the upstaging of the boundaries between public and private sphere. In fact, since nobody can neither perceive its gaze nor take shelter from it, the possibility of the individual to manage the projection of her identity fades away. Moreover, the global reach of this power makes it difficult to regulate, and therefore it is a reason of delegitimization of traditional politics. Yet, albeit it is a source of uncertainty because of the above mentioned features, surveillance works and it is widely perceived as legitimate. For Bauman and Lyon, this happens precisely because of the weakness of social bonds characterizing the contexts within which liquid surveillance successfully unfolds. In order to avoid isolation and the condition of vulnerability deriving from it, the individual accepts the surveillance enacted by digital platforms that connect her to other people: ‘to be always under control’ means ‘to be never alone again’. In this semantic shift utopia and dystopia merge, stating the legitimacy of absolute transparency as dominant social norm and fundamental design criterion of the digital daily tools. The only freedom inscribed in them is the one of being constantly exposed to the gaze of others and, therefore, to turn into a commodity on the bench of the global market.

The anonymous collective Invisible Committee (2019) formulated a similar analysis which can be summed up in the adage “the power creates void, the void calls the power” (ibidem, 149) coined by its members. According to the authors, if digital surveillance has been able to succeed, it is because it has unfolded in a historical context marked by a relentless dissolution of social bonds, being actively pursued by the rulers. In a scenario mainly marked by precarity, alienation, isolation and widespread insecurity, devices and platforms being developed by the Internet companies promise to grant anew the freedom of communicating, that is to say to put things "in common" with others. Yet, counter-intuitively, resorting to such freedom means to accelerate that dissolution of social bonds the power covets. Firstly, because the constant access to knowledge, services and people being provided by smartphones and social media produces an illusion of absolute autonomy that turns into a total dependency from these drivers. Secondly, because our freedom of communicating being inscribed in them is actually the premise of slavery: if information can circulate without obstacles, it is only because it does so in a transparent, and therefore controllable way. To save your own data in the cloud means to save your own government, that is, the government of ourselves, the one that we make possible by voluntarily providing a detailed database about our lives to those who hold power. This endless accumulation of information is at the foundations of the "practices of mass algorithmical control" (ibidem, 170) through which the cybernetic government knows, predicts and above all builds the behavior of the ruled. Squeezed between a total dependency from the digital infrastructures and their pervasiveness, the individual turns into a Quantified Self, that is a system-being inscribed in a complex tangle of computers: she lacks of autonomy because she is able to understand herself only starting from her exteriority, that is from the information produced about her by the machines to which she is connected. In order to rule over this subject – that is, to maximize her potentialities and direct her freedoms – it is sufficient to act on the technological environment through which she gives meaning to the world: to modify the variables of the context means to be able to alter the behavior of the individual present therein. Thus power has an infrastructural character: it is architectonic, immanent to the organization of life itself, and impersonal (which is why the representative function of politics fades away).

Also James Bridle (2019) asserts that the problem of digital surveillance must be analyzed with an infrastructural perspective. According to the scholar, the Internet is a "structure of knowledge and action" (ibidem, 24) that by now crucially mediates individuals' perception: as such, it affects people's ability to imagine the world, and therefore, to imagine their role within it. Bridle argues that the hypertrophy of knowledge being made possible by the web results in a drastic reduction of the mankind's agency, a paralysis of action that is reducing it in a state of passivity. This informative abundance is stimulated by the rise and diffusion of the "computational thought": a techno-determinist epistemological approach that presupposes an identity between the amount of information available to the individual and the quality of the decisions she is able to make. According to this rationale, every problem can be quantified – that is, described through the highest possible quantity of information – and solved through computation being operated by increasingly powerful machines. The idea that making something visible through a computer system equals to improve it is at the core of the Internet's principle of informative transparency which, according to Bridle, ushered a “new dark age”. Data overproduction proved to be unmanageable by human intellect, by bringing it to an overload: the result was a blackout, a general numbness which turned into an inability to thinking the world and therefore to act within it. Moreover, the blind trust towards the goals the technology was developed for (that is, data collection and processing), the total reliance we make on it in our daily life and the complete opaqueness of its functioning mechanisms brought us to a condition of total dependency that does not even allow to elaborate a critique of the forms of dominion it has established. Ultimately, the complete cultural, political and economic legitimization of surveillance has also brought social movements to reproduce its rationale: the whistleblower has become the new folk hero that everyone is waiting for, along with the information he is going to reveal in order to set people free. The excess of trust in the machines and information condemns us to inertia and produces a feeling of impotence that leads to paranoia and social disintegration.

Many of the aforementioned themes are brought back and formalized in Shoshana Zuboff’s "surveillance capitalism" paradigm (2019a). Surveillance capitalism is a market project that has the ambition of transforming the entire human experience in a commodity through a new logic of capitalist accumulation. Its main asset is the “behavioral surplus”, which is that personal set of data that – even when irrelevant for the purposes of the service being provided – are mined by the internet companies through an extensive surveillance of people’s activities (being them online or of offline). The behavioral surplus is then turned into “predicting products” able to directly intervene in consumers’ choices and, then, to produce behaviors that bring secure outcomes for the customers of surveillance capitalism (that is, advertisers). This happens through an automated architecture of extraction and execution, that is, through ubiquitous systems of data collection able to predict, modify, structure and manipulate human behavior. The "instrumentalizing power" of the "Big Other" (that is, of the surveillance infrastructure of the Internet) puts under attack individual autonomy with the aim of turning it into automation. Surveillance capitalism companies intervene in the processes of individual choice and aspire to replace freewill with a set of predetermined options, tailored in order to guarantee the advertisers to sell their products. Moreover, the right to decide whether an information should be public or not is unilaterally transferred to these same companies: the individual must be expropriated of her intimacy in order to optimize data accumulation. In this social and economic system there is no more reciprocity between rulers and ruled, since the latter are bound to the former by a condition of absolute dependence. In this dynamic, the premises of collective action (Zuboff, 2019b) are neutralized as well, since the digital is the core of social participation, but also the main supply chain of behavioral surplus: it is not possible to opt out from mechanisms being designed with the specific aim of nullifying personal awareness and there are no more trusted channels through which people voice can be heard.

1.3. Tor: a brief introductory overview

The Onion Router (which I will refer to with the acronym "Tor" from now on) is the object of this thesis. Tor is a low-latency, distributed and semi-centralized network operated on a voluntary basis and aimed to create an anonymous bi-directional communication channel. The open source software on which it is based was first publicly released in 2003, after its prototype underwent a long phase of experimentation and improvement, that started in the US Naval Research Laboratory in 1996. Tor has two main technical functions. First, when the Internet traffic is routed through the Tor network, it randomly bounces through a series of encrypted tunnels before reaching its final destination: in this way the sender of a communication cannot be associated with its recipient. In addition, Tor allows the creation of internet services (called 'onion services') capable of hiding the geographical position of the host server and resisting network disruptions provoked by hostile parties. According to the statistics provided by Tor Project[8], the network is used by 2.5 million users[9] on a daily basis and it is composed by 10.000 nodes[10] that provide a total amount of bandwidth corresponding to 400 Gbit/s[11]. The traffic generated by onion services is currently estimated at around 4 Gbit/s [12]. Interestingly, in the last ten years the traffic routed either by relays [13] and onion services[14] has greatly increased.

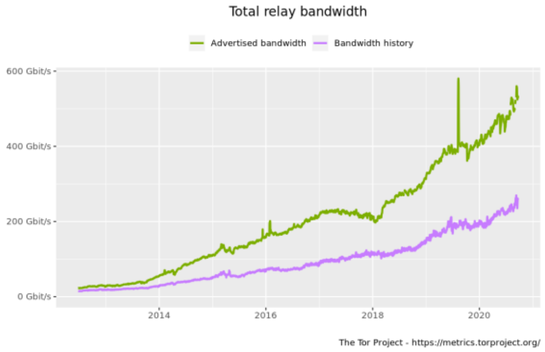

Fig. 1: Tor network bandwidth (2012-2020)

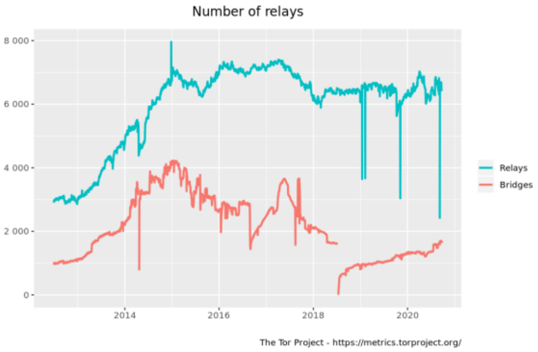

Fig.2: Number of Tor relays (2012-2020)

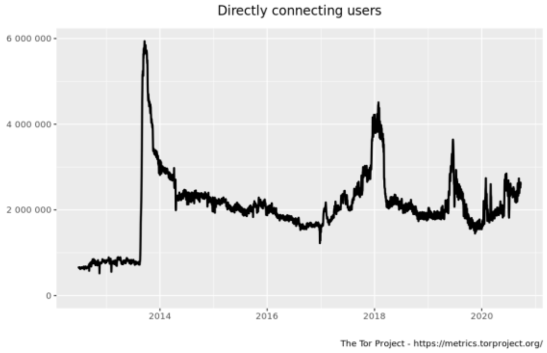

Fig. 3: Number of Tor users (2012-2020)

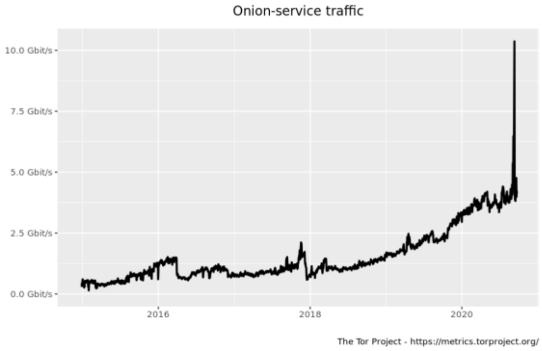

Fig. 4: Onion service traffic (2014-2020)

The community in charge of Tor development is formed by thousands of individuals and collectives that contribute in many different ways to its growth and maintenance. Tor is a very osmotic human aggregate characterized by different layers of participation. Its core is composed by the Tor Project Inc (TPI), a non-profit entity run by many volunteers and a few employees: hackers, software developers, security researchers, lawyers, translators, graphic designers and system administrators belong to it. Secondly, there are relay operators, people who run one or more nodes of the Tor network. They act as independent individuals or in membership groups, whose objective is to fund the development of the network and to increase its dimensions, performance and reliability. Thirdly, there are hundreds of hackers who develop the Tor ecosystem[15], that is a set of software with built-in anonymity features. The number of these projects is very high, and it involves a process of development going from mobile apps to browser add-ons, from instant messaging clients to complete operating systems. Finally, Tor is supported associations that provide funds, legal and technical assistance or advertising about the project. Electronic Frontier Foundation (EFF), Mozilla Foundation and Debian (the most widely used Linux based operating system) belong to it.

Tor is often celebrated as a tool for activists and journalist who live and operate in critical scenarios. Also, it has been a crucial infrastructure for a grassroots movement like Anonymous. Due to its capability to circumvent censorship it has become an optimal tool in many theaters of conflict (for instance the so-called "Arab Springs"[16], the 2014 Turkish Twitter blockade[17] or the Libyan civil war[18]). Its open source code has been the basis for the development of several whistleblowing platforms[19], adopted both by international newspapers concerned with the protection of their sources and by NGOs being actively involved in exposing government corruption. Free from geographical constraints, its environment has been used to conduct illegal activities: Tor is often associated with the infamous Silk Road, and more in general with on-line black markets which are only accessible through it. However, the anonymity provided by Tor is far from being employed merely for unlawful ends. Indeed, its functionalities and security properties are being increasingly employed by IT companies (Facebook[20] [21], Cloudflare[22] [23] and Mozilla[24] [25] [26] are just the most prominent ones), global media outlets (like the BBC[27], the New York Times[28] or the Deuschte Welle[29]), government agencies (for instance the US Central Intelligence Agency[30]) and players belonging to the adult entertainment industry (Pornhub[31]) as well. In short, Tor is used by common people, military forces, law enforcement officers, business executives, companies, bloggers and IT professionals as well as activists, journalists, and criminals. The forms of communication made possible by its code have drawn the attention of a plurality of organizations that are very different and apparently irreducible to one another. In all respects Tor can be considered as an invisible background for "pervasively enabling resources in network form" (Bowker et al 2010, 98), thus supporting practices, social

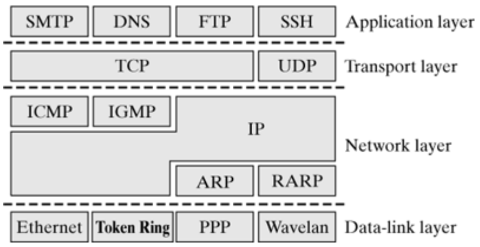

Fig. 5: The Internet Protocol Suite

experiments and forms of communication arisen in response to the ubiquitous state of surveillance that the Internet is facing today. Yet, at the same time, the Tor network is also used by those same actors (Facebook, above all) who, as we have seen in the previous sections of the chapter, are directly responsible for this state of affairs.

In order to understand this apparent contradiction and to make emerge the plurality of interests characterizing Tor, it is necessary to trace back its origin or, more precisely, the multiplicity of its origins. Indeed, as any other infrastructure, Tor is made up of a plurality of contexts, stories, practices, actors and unexpected encounters that gave life to it. In order to unravel this intricate tangle, I have decided to follow Sandvig's suggestion (2013, 93) and to start the exploration of Tor infrastructure by setting a "useful entry point", that is a moment that allows to put in relation the past with the present and brings to light the elements that still shape the way we use and think a technology. This is entry point is the RFC 791.

1.4. RFC 791: a standard entry point

Released on September 1981 by the IETF – about fifteen years before the development of Tor started – the Request For Comments[32] (RFC) 791 (Postel, 1981) is a forty-five page long document defining the technical properties of the Internet Protocol (IP). Edited by Jon Postel – a legendary figure in the Internet culture, known not only for his tireless dedication to the maintenance of the Internet name server system, but also for his opposition to its return under the control of the US military in 1998 (Goldsmith and Wu 2005, 31-50) –, the RFC 791 was actually the result of more than three years of work by many contributors[33].

Before analyzing the RFC 791, it is important to point out that the IP is only one among the thousand of protocols created with the aim of providing interoperability between different types of technical devices running over the Internet. Such protocols are organized into the “Internet Protocol Suite”, a conceptual hierarchical scheme built on four communicating interfaced layers, each of them being built on the top of the other. The first layer is the ‘data-link layer’: the protocols belonging to it define the physical link through which different computing devices are connected. In this layer we can find protocols such as Wi-Fi, Ethernet, 4G, GSM, NFC or Bluetooth. The second layer is the ‘Internet layer’: the IP is the only protocol being present on this layer. The third layer is the ‘transmission layer’. The protocols within it – that is the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) – are aimed at verifying that data are correctly transmitted between two different nodes of a network. Finally at the ‘application layer’, the forth one in the Internet Protocol Suite, we can find the protocols which directly interact with the applications being used by a computer. Among these protocols we can mention HTTP, DNS, SMTP, FTP, POP, XMPP and many more.

In order to understand why the IP is crucial for Tor’s history we need first to look at its goals and design principles. The IP has been designed in order to bridge many heterogeneous autonomous ‘packet-switched’ computer networks into a single meta-network (that is, the Internet). In other words, its goal is making different networks and local protocol implementations inter-operate without a centralized control. The IP is in charge with ‘routing’, that is the process of defining a transmission path between two different computers so that they can exchange ‘datagrams’ (or ‘blocks of data’ or ‘packets of data’). The computers present in an IP-based network are identified by a univocal numerical label called ‘IP address’ being assigned to each of them. An IP address is a number expressed in fixed length of four octets, which indicates where a computer or a network resource is located. In order to communicate with other devices, a computer must be provided with an IP address. Since the IP fulfills this fundamental function and, as we have seen above, it is the only protocol present on the Internet Protocol Suite network layer, it has a character of universality, namely it is “a necessary precondition to being on the Internet” (DeNardis 2009, 9).

Distribution is the most relevant design principle of the IP. Indeed, routing instructions reside in each computer and “gateway” – that is computers connecting different local area networks (LAN) – through which traffic moves. In this sense, the IP is ‘end-to-end’:

it does not rely on a central authority for the delivery of data, but on already existing local network protocols. Indeed, in an IP-based network a datagram is carried from a node to another, until it reaches the destination host. In other words, in the Internet architecture "intelligence (that is to say data processing) is situated only at the ends, thus decentralizing the load and freeing the network from heavy tasks" (Carlini 2002, 19). This approach to networking has been defined as "stupid" (Isenberg 1997) – since the responsibility for control over data is relocated from the infrastructure to the nodes being situated at its ends – and "transparent" or "oblivious" – since the infrastructure that transmits the traffic "does not filter or transform the data that it carries" (Aboba and Davies 2007, 1). Also, the end-to-end design principle makes the IP robust (that is, resistant to outages). Indeed, if the hop of a route is out of order for any reason, a gateway can process autonomously an alternative route in order to deliver a datagram to the destination host. Finally, it is worth noting that the IP distributed nature in turn made the creation of heterogeneous networks possible: indeed, it drastically reduced the complexity of adding new services and applications to a network and, also, it made possible to do so without having to change its core or asking someone permission.

Design principles such as distribution, robustness and heterogeneity were embodied into the original Internet architecture because of a plurality of reasons. In part, such principles originated from the fact that Arpanet "was designed to operate in a military context, which implied the possibility of a hostile environment" where survivability of the network was paramount, whereas the accountability of its resources was not a relevant priority[34] (Clark 1988, 103). On the other hand, such design principles mirror the original hacker culture, born as a form of reaction to the Cold War historical context, within which any form of individualism was squashed between the Fordist production system – characterized by processes of monopolistic concentration, bureaucratization of the enterprise and centrality of the State in the mediation of the social conflicts – and a broadcast media apparatus built for co-opting masses in the consumption system and mobilizing them through propaganda (Formenti 2006, 47-60). In response to this situation, the earlier Internet engineers tried to conceptualize a medium that, rather than rationalizing and centralizing the information flow into the hand of a single entity, could foster decentralization, autonomy, self-determination and freedom of use.

Furthermore, such design principles have been major factors for the global success and the rapid growth of the Internet. More specifically, they have been paramount in the formation of a digital marketplace scattered on a global scale. For instance, in the 1980's, when the adoption of computers at a corporate level began to spread, heterogeneity proved to be crucial. At that time, technological enthusiasm that accompanied the diffusion of the first personal computers had led many business executives to purchase digital equipment without following a specific criterion for integrating it effectively into the working environment (Edwards 1998, 22). This resulted in offices being jam-packed with incompatible, stand-alone machines and unsuitable software for sharing data (DeNardis 2014, 68). After this chaotic start, the inter-connectivity and openness characterizing the Internet protocols allowed managers to integrate heterogeneous networks within a single technological framework and reassert an administrative control over the data of their companies (Rochlin 1997).

Therefore, like any other medium, the Internet is essentially a space for action: its main peculiarity is that of connecting what is separate (Zielinsky and Custance 2006) through a series of agreements on how to move data between two points (Shirky 2010). Yet, as rightly noted by Couldry (2015, 6), it cannot be considered only as a platform for individual discovery and collective contact, but also – as we have seen in the previous sections of the chapters – as a tool for mutual surveillance. How did a distributed stupid network, being designed to be oblivious to users' communications, become an intelligence tool employed for mass surveillance? In order to answer this question we need to focus our attention on the IP technical specifications.

1.5. Is it a feature or a bug?

As explained above, the IP is essentially a set of rules for sending datagrams from a local network to another. Datagrams are made by two distinct elements. The first one is the 'payload', that is to say the part of the packet carrying the data. The second one is the 'header', made by a variable number of bits where different information – like the length of the datagram measured in octets, the Time to Live[35], the Type of Services[36] – are stored. Among the values encoded into the header, there are two relevant parameters which need to be mentioned for the purposes of this thesis, namely its ‘source’ and its ‘destination’, both of them being identified by their ‘IP addresses’.

IP addresses are crucial information required by gateways in order to create a ‘route’ between end-points, that is to provide them with a path to follow for transmitting datagrams from a sender to a recipient. Every time a datagram arrives to a gateway, this latter reads its source and destination address. According to such information, the gateway determines the next gateway to which the packet of data is to be forwarded. This process occurs from gateway to gateway, until the packet reaches the destination host. It is important to emphasize that, according to the IP technical specifications, routing always requires the identification of the parties involved in the process. This means that IP addresses identifying the sender and the recipient of a datagram are known to each single gateway through which a packet of data is moved. In plain words, the IP rules establish that the process of routing and the process of identification of the hosts involved in the communication are not separate.

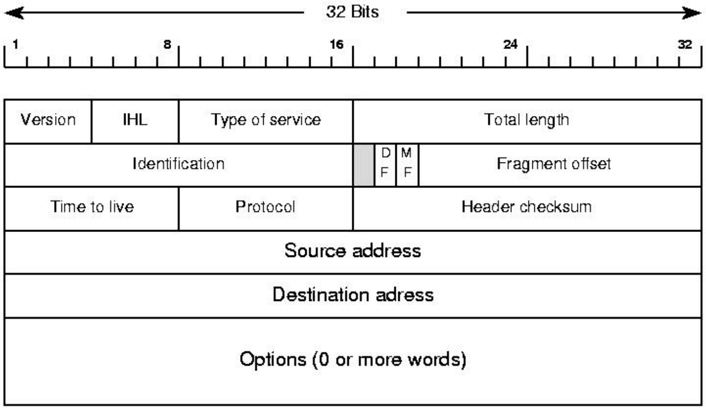

Fig.6: Internet Datagram Header Structure

The overlapping of these two functions has a crucial side effect: *a public IP-based network reveals by default who is talking to whom*. In other words, it does not provide *routing confidentiality*. Indeed, a hypothetical actor who controls (or has the power to observe) a gateway that connects two or more different local networks can easily track down the packet route by simply reading the source and destination IP addresses encoded into the header. In this way she can identify the location of the parties involved in data exchange and infer information from the communication pattern. For instance, she can see when they talk to one another, the frequency of their communication, its duration and the volume of data being exchanged. Furthermore, IP does not provide *traffic authentication*, that is, it does not ensure that the person (or site) with whom one is exchanging data is actually who (or what) it claims to be. Indeed, an actor who controls a gateway not only can read the datagram header, but she can also manipulate it and hijack the traffic to a different receiver than the one the sender wants to talk to, without this latter can even notice. Also, IP does not even guarantee *traffic confidentiality*. Since datagram payload is not encrypted, nor protected by any mean, an observer can intercept the content of the communication, as well as manipulating it, and even then without the receiver being able to realize that. Yet, it is worth noting that payload encryption does not make harder to understand who is talking to whom: since datagram header remains in clear text, communication sender and receiver can be always observed, as well as timing, frequency and volume of the data they exchange.

Fig. 7: T/A. When you encrypt the payload but not the header

With an analogy, we could say that the functioning of IP resembles very much the rules of a children's game being called in Italian “telefono senza fili” (literally “wireless phone”) and in English “Chinese whispers”. During the game, its participants (in our analogy, end points and gateways of the network) must be arranged next to one another until they form a row (that is to say, the network). The first kid in the row covers her mouth with the hands and whispers a sentence (the datagram payload) and the name of the recipient (the datagram header) in the ear of the kid closest to her. In turn, the second kid whispers the same phrase in the ear of the kid who is closest to her along with the name of the sender and that of the recipient (he acts as a gateway). Then the third does the same and so on. After a series of steps, the message is delivered to the recipient who must shout it aloud in front of everyone[37]. Every kid playing the game knows who is the initial sender and the final recipient of the message (this is routing confidentiality). Each of them knows the content of a message and has the power to change it (traffic confidentiality), as well as the name of the recipient (traffic authentication). Also, a person who observes the group of children playing will not be able to know what kids are whispering to one another. Nevertheless, she will always know who sent the message to whom.

As it happens for the wireless phone, the IP is efficient when it comes to quickly and easily move a message. However, it is not designed to protect routing and confidentiality, nor to ensure traffic authentication. A third party can easily interfere with the communication between the nodes of a network and/or monitor them. The information gathered can be later analyzed in order to infer several types of information about the parties involved in the communication. This is a communication intelligence (COMINT) technique called traffic analysis (T/A).

1.6. Traffic analysis: exposing the enemy's skeleton

T/A was not born with the Internet but it has ancient roots in military culture. Its origins have been investigated by David Khan in "The Codebreakers". Published in 1967, this book is still considered as one of the most relevant work in the history of cryptology and looks at the evolution of military information networks since the 19th century. Echoing McLuhan's approach in "Understanding media", Khan frames the technological developments occurred in this field, not much in terms of increased operability of the troops on the battleground but rather as forces transforming the same battleground and, in turn, the whole idea of war as part of the human experience. By analyzing the role of telegraph and radio in armed conflicts, the scholar observes two linked phenomena. First, he explains that the more the human capability of communicating is amplified by a media, the more are the possibilities that information communicated through it is intercepted by a third party. Second, he claims that in turn this transformation entails a drastic change in the organizational mechanisms and practices for waging war.

> "Just as the telegraph had made military communication much more effective but had also increased the possibility of interception over that of hand-carried messages, so radio's vast amplification of military communications was accompanied by an enormously greater probability of interception. The public, omni-directional nature of radio transmissions, which makes wireless communication so easy to establish, makes it equally easy to intercept. It was no longer necessary to gain physical access to

> establish access to a telegraph line behind the enemy's front to eavesdrop upon his communication. A commander had only to sit in his headquarters and tune to the enemy's wavelength" (Khan 1967, 151).

T/A has been the result of the above mentioned historical shift. Along with crypt-analysis (C/A), T/A is one of the most prominent approaches to COMINT. T/A has been employed as early as the American Civil War but it assumed high relevance only during WWI, when radio started to be employed for military purposes (Borrmann et al 2013, 10). As mentioned in a NSA memorandum dated 1954, this intelligence practice is "dependent primarily upon the existence of radio communication" (Benjamin 1954, 3).

T/A is the study of traffic – that is the communication passed between a sender and intended recipient – by an external observer who is scanning it for patterns like: what is the frequency of the communications? How does this frequency change over the time? Who is talking to whom? When do people talk? Where are the senders located? Has their location changed? In other words, T/A is not focused on the content of an intercepted dispatch – since it is often protected with a code and, as such, it is unreadable – but on gathering information from elements external to it. When they are correctly interpreted, such 'externals' are particularly important for intelligence operations because they can provide a sort of snapshot of the enemy's communication network structure. Elements such as net structure, traffic volumes, traffic contacts or traffic patterns represent valuable information in order to decipher the adversary's 'order of battle' – namely a military unit's identification, organization, strength and location –, to identify its capabilities, to monitor its troops, to understand their deployment and to predict their plans (Borrmann et al 2013, 5). "The organization of a radio network" claims Callimahos (1958, 2) "and the manner in which messages are passed over this network reflect troop disposition, command relationships, and impending movements and preparations for military activity". For instance, a Navy vessel receiving the higher volume of radio signals is usually the flagship. Or, the increased volume of traffic between ships is almost always the sign of an operation underway and announces an imminent attack. Also, radio signals are great indicators of ship position, course and speed. In Khan's words, T/A "maintains a long-range, invisible, and continuous surveillance of fleet movements and organization, providing a wealth of information at low cost" (Khan 1967, 14). Another way for describing T/A is the enlightening metaphor being provided by Alexander Powell (1919, 21), an American war correspondent and military intelligence captain during WWI:

> "Just as naturalists can reconstruct from a few bones a prehistoric monster, which they had never seen, so the goniometric experts are able to gain an amazingly accurate idea of the organization of an army by locating its stations, for the lines of radio communication, which spread fan-wise from the headquarters, form a sort of skeleton, as it were, of the army's organization, the location of the various stations and their distance from headquarters indicating quite accurately the position of the corps, divisions, brigades, regiments, and battalions".

In one sentence we could say that T/A tries to investigate an object internally by looking at it externally[38].

In T/A – and more in general in COMINT – one of the most important and problematic variable to be taken into account is the amount of collected data (Giannuli 2013). Indeed, T/A usually becomes more effective with the growth of the information being gathered. At the same time though, the more is data being collected, the more is the complexity to give it a meaning and to get a human-readable output from it. In order to be solved, this problem requires proper models for interpreting data and the support of an adequate human interface: indeed, the successful implementation of any machine, independently of its level of sophistication, always relies on disciplined human beings (Edwards 2004, 828). Without these elements, a T/A operation can easily become a failure: as explained by Bridle (2019, 203-4), in recent years the excess of intelligence generated by the US global surveillance dragnet is “flooding analysts, making it impossible to track relevant data in order to address specific threats”.

1.7. An unintended consequence

Paraphrasing Khan's previous words, we could say that the vast amplification of communications made possible by the IP entails a significant increase in the probability that they will be intercepted and analyzed. The global reach of the Internet and its design make it as easy to establish communication between two points as to monitor it. This because of two reasons. First, because with the increase of the checkpoints communication pass through, the possibility it could be intercepted increases as well. Second, because the IP protocol is concerned "only with the efficient routing and addressing necessary for the packet to reach its end point" (DeNardis 2009, 10) but not with the confidentiality of the process.

However, it is worth emphasizing that T/A is not a feature originally planned in the IP. On the contrary, it can be considered as a bug, a flaw in its design and hence, an unintended consequence – one unforeseen by its creators. The emergence of unintended consequences is a historical dynamics of technological development: every single technology that we use on a daily basis is (or was) affected, at least, by one unexpected consequence (Tenner 1997). Solving unintended consequences is the true essence of technological development: it is a process that requires years of background work and involves a large amount of scientists and engineers. An unintended consequence can have several culprits: a flaw in the design of a technology, a use of it which had not been foreseen by its creators, or a purpose for which it can be used that they could had never imagined when they had developed it. The more a technology is successful, the more serious are the problems being created by its unexpected effects. It is not uncommon for a feature to become a bug and to give rise to unintended consequences. This is true for many fundamental components of the Internet such as the Domain Name System (DNS) (Bradshaw and DeNardis 2019), the Network Time Protocol (NTP) (Edwards 1998) or the IP.

The emergence of T/A on the Internet mirrors the above described dynamics. First of all because the overlapping of routing and identification planned in the IP technical specifications is not necessary by any mean for the correct functioning of the Internet infrastructure. As stated in 1997 during the seventh Internet Society conference (ISOC) by Michael G. Reed, David Goldschlag, and Paul Syverson (1997) – civilian employees at the US Naval Research Laboratory (NRL) and creators of the Onion Routing (OR) protocol on which Tor is based – "there is no reason that the use of a public network like the Internet ought to reveal to others who is talking to whom and what they are talking about". According to Paul Syverson[39], this is an unintended consequence that the creators of the IP could had never foreseen (and, even if they did, it would have been hard to reach an optimal solution to fix it).

> "Like so many things, if you are designing just to make something work and then you after the fact you think of some of the security properties… I mean… I do not think they had taught about how they had even confidentiality and authentication for the data, much less authentication and confidentiality for the routing, which was you know what we did. Initially you just try to get the things to communicate well. […] So I think it was just the easiest way to get something from one place to another and then you think "oh wait, now I want to protect that information of where I am going and where I came from, so how I do that?" […] This is always the hard thing. Partly you could say "People weren't thinking" but the truth is it's often hard to understand if you come up with a new brand technology, you can think to the security from the ground up, but understanding what kind of threats and what sort of thing you should try to build in, even when you think about it, it can be very hard to get an adversary model and that sort of things right. In insight we can always see "oh, we should have done this and that" but it's hard… it is always easy to say "why didn't they do this?", but it is not so easy to know what things to add and what not".

The technical community involved in the development of the Internet has reached a broad awareness of the general dynamics described by Syverson, and has even formalized it in the RFC 1287. According to the document "experience has shown that it is difficult to add security to a protocol suite unless it is built into the architecture from beginning" (Clark et al. 1991, 3). But embedding security from scratch into a protocol is not always easy, as explained by one of the TCP protocol creators, Vinton Cerf. In an interview released in 2014[40], Cerf claimed that if he could go back to the past and change something in the original Internet architecture then he would add public key encryption. According to the engineer, in the early 1980s this option was actually on the table but several issues related to its technical implementation – such as the lack of a suitable algorithm for deploying asymmetric encryption or the impossibility to scale an already existing solution provided by the National Security Agency (NSA) – eventually made it unpractical.

Furthermore, the fact that the Internet architecture was developed in a completely different historical period than the current one is among the main reasons for its persisting insecurity issues. Indeed, "although military security was considered when the Internet architecture was designed, the modern security issues are much broader, encompassing commercial requirements as well" (Clark et al 1991, 3) which were not considered at all in its original design (Clark 1988, 103). The early Internet was not characterized by widespread commercial or social interests and it "was designed in simpler times, when the user community was smaller. It was reasonable to trust most of the users, and it was possible to track down and deal with misbehavior" (Clark et al 2005, 93). Because of this reason, it was built according to criteria of information transparency and public access and it "did not have the type of security and privacy features modern systems include" (Bradshaw and DeNardis 2019, 20) and that contemporary global Internet requires.

1.8. The CHACS

Tor can be considered as a reactive protocol: it is born for solving an unintended consequence (namely, T/A) provoked by another technology (that is IP) that its creators had not been able to foresee. In metaphorical terms, Tor is a patch for fixing (or at least mitigate) one of the many bugs affecting the Internet since its origins. Who did decide to develop it, and why?

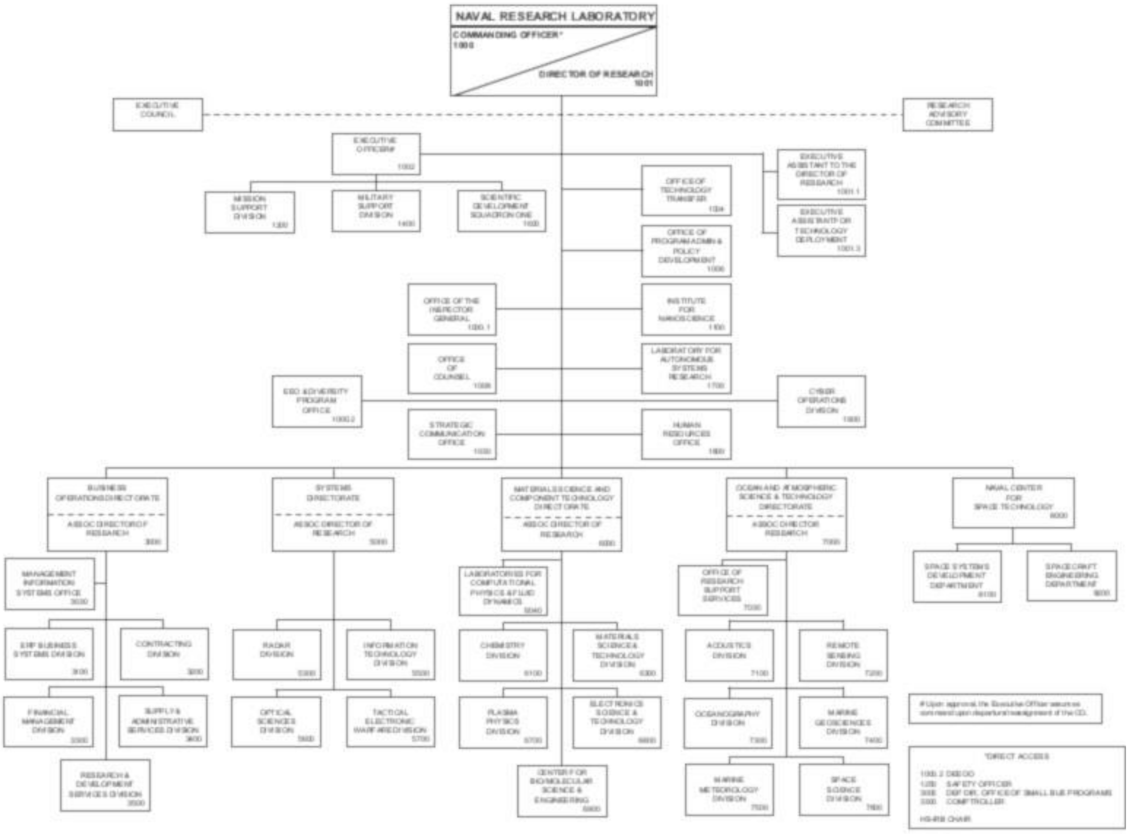
NAVAL RESEARCH LABORATORY
COMMANDING OFFICER* 1000
DIRECTOR OF RESEARCH 1001
EXECUTIVE COUNCIL
RESEARCH ADVISORY COMMITTEE
EXECUTIVE OFFICER# 1002
MISSION SUPPORT DIVISION 1200
MILITARY SUPPORT DIVISION 1400
SCIENTIFIC DEVELOPMENT SQUADRON ONE 1600
OFFICE OF TECHNOLOGY TRANSFER 1004
OFFICE OF PROGRAM ADMIN & POLICY DEVELOPMENT 1006
EXECUTIVE ASSISTANT TO THE DIRECTOR OF RESEARCH 1001.1
EXECUTIVE ASSISTANT FOR TECHNOLOGY DEPLOYMENT 1001.3
OFFICE OF THE INSPECTOR GENERAL 1000.1
INSTITUTE FOR NANOSCIENCE 1100
OFFICE OF COUNSEL 1008
LABORATORY FOR AUTONOMOUS SYSTEMS RESEARCH 1700
EEO & DIVERSITY PROGRAM OFFICE 1000.2
CYBER OPERATIONS DIVISION 1300
STRATEGIC COMMUNICATION OFFICE 1030
HUMAN RESOURCES OFFICE 1800
BUSINESS OPERATIONS DIRECTORATE
ASSOC DIRECTOR OF RESEARCH 3000
SYSTEMS DIRECTORATE
ASSOC DIRECTOR OF RESEARCH 5000
MATERIALS SCIENCE AND COMPONENT TECHNOLOGY DIRECTORATE
ASSOC DIRECTOR OF RESEARCH 6000
OCEAN AND ATMOSPHERIC SCIENCE & TECHNOLOGY DIRECTORATE
ASSOC DIRECTOR RESEARCH 7000
NAVAL CENTER FOR SPACE TECHNOLOGY 8000
MANAGEMENT INFORMATION SYSTEMS OFFICE 3030
ERP BUSINESS SYSTEMS DIVISION 3100
CONTRACTING DIVISION 3200
FINANCIAL MANAGEMENT DIVISION 3300
SUPPLY & ADMINISTRATIVE SERVICES DIVISION 3400
RESEARCH & DEVELOPMENT SERVICES DIVISION 3500
RADAR DIVISION 5300
INFORMATION TECHNOLOGY DIVISION 5500
OPTICAL SCIENCES DIVISION 5600
TACTICAL ELECTRONIC WARFARE DIVISION 5700
LABORATORIES FOR COMPUTATIONAL PHYSICS & FLUID DYNAMICS 6040
CHEMISTRY DIVISION 6100
MATERIALS SCIENCE & TECHNOLOGY DIVISION 6300
PLASMA PHYSICS DIVISION 6700
ELECTRONICS SCIENCE & TECHNOLOGY DIVISION 6800
CENTER FOR BIO/MOLECULAR SCIENCE & ENGINEERING 6900
OFFICE OF RESEARCH SUPPORT SERVICES 7030
ACOUSTICS DIVISION 7100
REMOTE SENSING DIVISION 7200
OCEANOGRAPHY DIVISION 7300
MARINE GEOSCIENCES DIVISION 7400
MARINE METEOROLOGY DIVISION 7500
SPACE SCIENCE DIVISION 7600
SPACE SYSTEMS DEVELOPMENT DEPARTMENT 8100
SPACECRAFT ENGINEERING DEPARTMENT 8200
# Upon approval, the Executive Officer assumes command upon departure/reassignment of the CO.
*DIRECT ACCESS
1000.2 DEEO
1200 SAFETY OFFICER
3005 DEP DIR, OFFICE OF SMALL BUS PROGRAMS
3300 COMPTROLLER
HS-RB CHAIR

Fig. 8: NRL's organizational chart

The answer to the latter question is complex and it requires an elaborate reasoning. Tor has many roots and some of them are deeply entrenched in the US military institutions that historically played a pivotal role in the establishment of the Internet (Edwards 1996; Castells 2002; Mazzucato 2018; Bridle 2019). The creators of the OR upon which the Tor infrastructure is based are Paul Syverson, David Goldschlag and Michael Reed. In 1995, when the Office for Naval Research (ONR) provided them with the first funding for OR development, they were working as civilian employees in the "Formal Methods" section of the Center for High Assurance Computer Systems (CHACS), a NRL's Information Technology Division (ITD) research branch.

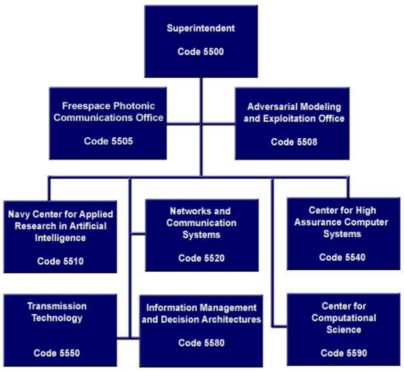
Superintendent
Code 5500
Freespace Photonic Communications Office
Code 5505
Adversarial Modeling and Exploitation Office
Code 5508
Navy Center for Applied Research in Artificial Intelligence
Code 5510
Networks and Communication Systems
Code 5520
Center for High Assurance Computer Systems
Code 5540
Transmission Technology
Code 5550
Information Management and Decision Architectures
Code 5580
Center for Computational Science
Code 5590

Fig. 9: NRL ITD's organizational chart

The NRL is one of the most important government research center in the US. Affiliated with the Navy, it has 2600 employees (mostly civilian scientific researchers) and an annual budget of one billion dollars[41]. According to its home page, the ITD was established in order to conduct basic research, exploratory development, and advanced technology demonstrations in the collection, transmission, and processing of information in order to provide a basis for improving the conduct of military operations[42]. ITD is organized in eight offices among which there is the CHACS. This research center specifically deals with High Assurance Computer Systems (HACS), that is, computer systems featuring four critical priorities:

a) “security” (HACS must prevent any form of unauthorized disclosure, modification and withholding of sensitive information),
b) “safety” (HACS must avoid unintended events resulting in death, injuries, illness or damage of property),
c) “real-time” (HACS must deliver results within specified time intervals),
d) “fault-tolerance” (HACS' quality of service must be guaranteed in spite of possible faults).

The CHACS' mission is that of developing experimental technologies equipped with these features, in order for them to be subsequently implemented in civilian, commercial or military infrastructure: flight control systems, medical and financial databases, information networks. CHACS is structured into six sections[43] among which the “Formal Methods Section” (FMS) whose mission is “to perform research on extensible and adaptable foundational theories that can be applied to present and emerging security problems”[44]. FMS’ research interests vary from cryptography to steganography, from distributed systems to informatics phenomena, up to including secure and anonymous communications.

It should be no surprise that the CHACS is where Tor was born. Given the previously illustrated importance of the concept of traffic analysis in military culture, it seems to be just obvious that the vast majority of the initial funding and resources being used for the OR development were supplied by a government laboratory with strong ties with the Navy. It is even less surprising when considering that the ITD is a direct heir of the NRL Radio Division, established in 1923 with the mission (among others) to research new and more efficient methodologies of radio traffic interception and analysis. Yet, there are other reasons because of this particular branch of US government spent time, money and resources in order to solve the problem of T/A. Already in the first half of the '90s, the CHACS formalized and published its own research agenda. The goal being pursued by such agenda was that of developing technological prototypes designed in order to secure the US digital infrastructure (McLehan and Heitmeyer, 1995). The strategy to achieve this objective was based on two simple assumptions. First, CHACS' scholars observed that market players would have never committed to this endeavor because of its lack of profitability in the short term; also, they remarked that the academy did not have the required resources to address it. Second, they emphasized how in the long run a lack of public intervention in dealing with this problem would have played out as a disaster, since the increasing dependence of the national system on digital infrastructures had made them “in effect, military targets” (ibidem 1995, 3). In order to prevent such scenario, the CHACS worked towards the development of experimental technologies based on new theoretical-conceptual models which had emerged in the cybersecurity research field, but that were still lacking of a practical application in real world. It was an ambitious goal: indeed, at that time there were neither computer systems featuring the four critical properties in order to realize a HACS, nor specific methods for building them. In order to reach such challenging milestone, the CHACS' experts claimed, it was necessary “to lead this research into the development community” and “to develop industry quality supporting tools to apply existing research methods on real systems” (ibidem, 8). The concocted prototypes would have then to be transferred to the private sector, in order for it to develop them on its own by realizing technologies being compatible with industrial standards and implementable within private infrastructures. Therefore, the CHACS committed itself to be a bridge able to connect government research labs, academy and industry.

The creation of OR fully matches the fundamental assumptions of this rationale. The research of Syverson, Reed and Goldshlag was actually inspired by the concept of 'Mix-net' being theorized by Chaum (1981) whose application was until then limited to the field of ISDN phone networks (Pfitzmann et al 1991) and email communications (Gülcü and Tsudik 1996). However, unlike these projects, OR was designed to work on the Internet and, more specifically, to work with low-latency protocols, like the Hyper Text Transfer Protocol (HTTP) on which the then emerging World Wide Web was based. Moreover, as we will see later in the chapter, among the goals listed in the first Tor design paper (published in 2004) there was exactly that of turning the infrastructure into an experimental platform in order to test the OR implementation on a mass scale and in real world. In addition, it must not be forgot that 25 years after the inception of the project, there have been dozens, if not hundreds organizations that contributed to its development: nevertheless, the only one who have had a steady presence and carry on to significantly contribute to the core of the Tor protocol, is actually the NRL. Finally, as we will see in chapter 3, Tor has become a technology which have been integrated in several platforms and ecosystems developed by the main important players in the ICT sector.

1.9. Network Centric Warfare

Another US military institution that initially contributed to the development of Tor is the Defense Advanced Research Project Agency (DARPA). Contextually with the rise of a new strategic military doctrine named Network Centric Warfare (NCW), DARPA invested lot of resources in the development of networks for Information Assurance and Survivability (IA&S), that is, communication infrastructures able to remain operative even in case of non-optimal conditions, determined either by enemy attacks and/or hardware or software failures. The AI&S technological development was ensured through the institution of numerous funding programs, including the Fault Tolerant Network Program (FTN), from which also the Tor developers benefited between 2001 to 2004[45].

The NCW can be defined as the stage of full technological maturity of the so-called Revolution in Military Affairs (RMA) developed in the 70’s. RMA entailed the reorganization of the US armed forces and it was devised as a mean for the strategic containment of the Soviet Union in the event of a conflict in Central Europe. Beside the availability of high-precision, medium-range weapons systems, the concept of ‘information superiority’ – that is the ability to share information in real time – is at the heart of RMA (and then of the NCW). Indeed, according to this doctrine, collecting, processing, protecting and distributing a relevant and accurate amount of information in a timely way – and at the same time denying such possibility to the opponent – is a key element to ensure a situational awareness of the operations theater and gain a strategical advantage over the competitor (Badialetti and Giacomello 2009, 208). The RMA's doctrinal notions were put into practice only during the first Gulf war and, once their effectiveness on the field was verified, they were subjected to further elaboration that will lead to the introduction of the concept of NCW (Cebrowsky and Garstka 1998) and to its following formalization (Alberts and Hayes 2003). The NCW entails that information superiority can only be achieved through an adequate communication structure which, therefore, must be placed at the center of the military organization process. Platforms, systems, concepts, everything must be planned and designed as a function of a network to which armed forces are connected as nodes. The sharing of information among the troops enables information awareness of the situation on the field, that turns into a greater efficiency of the operations being led.

In order to turn this vision into reality, in 1998 the United States started to build the Global Information Grid (GIG), that is a global infrastructure being finalized to the access and exchange of information, as well as to the sharing of intelligence among troops on the ground (Batocchi 2006, 21). Since the NCW called for a reorganization of US forces that would have made them *de facto* dependent on the network, it was absolutely necessary that this latter could keep providing a seamless flow of communications, even in the event of an enemy attack. For this reason, the GIG had to be built resorting to new generation technologies and protocols able to guarantee “information assurance”, otherwise known as “cybersecurity”. The institutional entity responsible for the development of these technologies is the DARPA's Information Technology Office (ITO) which in those years launched four funding programs: Critical Infrastructure Protection (CIP), Composable High Assurance Trusted Systems (CHATS), Dynamic Coalitions (DC) and Fault Tolerant Network (FTN)[46]. This latter focuses on three areas to be studied and evaluated: (1) fault tolerant survivability, (2) preventing denial-of-service attack, and (3) active network response. The FTN's call for applications – published by DARPA in December 2000 under the label "SOL BAA 01-22" and providing a 36-months worth funding – aimed at creating prototypes "that support continued network operations in the presence of successful attacks […], reduce the amount of damage sustained during an attack, and allow the network to maintain an acceptable, minimum level of functionality". Moreover, as explained in 2003 by Tony Tether (former DARPA director) during an audition held at the Scientific Committee of the House Of Representatives about the concept of Information Assurance[47], the networks being employed for the NCW should have been provided with another particular feature: they should have been assemble and reassemble "on-the-fly on an ad hoc basis without having a fixed or set infrastructure in-place".

As we will see in the next sections of the chapter, Tor precisely matches these features. Its distributed architecture (and the lack of a center of gravity underpinning it) requires an opponent to destroy the entire network in order to stop its communication. Actually, even if under a partially hostile control, the Tor infrastructure keeps working and guarantees both operativity and security of the information flow. Moreover, once set, onion services are accessible in an ubiquitous way and without the need for them to be reconfigured accordingly to the network they are on. Finally, as they do not have an IP address, onion services are resistant to specific kinds of attacks known as Distributed Denial of Service (DDOS) aimed at exhausting the resources of a system and making it unavailable (National Research Council 2000, 212).

DARPA seems to have had a crucial importance in supporting the construction of OR[48]. Indeed, in 1999 the development of the infrastructure had been suspended, partly because of the lack of funds, partly because its main developers had left the NRL. Moreover, in January 2000 the proof-of-concept OR network being built until that moment had been shut down while other anonymity-oriented networks (like JAP, created by the Technische Universität Dresden, the Universität Regensburg and Privacy Commissioner of Schleswig-Holstein) were coming up. Tor development resumed only in 2001, and it did because of the funds provided by DARPA. In 2003, the project received three distinct donations (one from ONR, one from DARPA and one from NRL) being aimed at reaching three different objectives: ONR's donation was about development and deployment of Tor code, DARPA's one was for building in resource management and fault tolerance, while the latter had been given for the creation of survivable onion services (at that time still being called 'hidden services').

It is also worth noting that, although they were not financially supporting it, many other institutions belonging to the US military apparatus had expressed interest in the development of the protocol. In a 1997 DARPA report written by Paul Syverson[49], – at that time the agency was funding the project under the High Confidence Network Program – it is explained that the Carnegie Mellon University, the Pacific Northwest National Laboratories and the NSA "have expressed interests in running a site" based on OR.

1.10. Why the government needs anonymity

Beyond the strategical frameworks within which Tor's development is situated, it is necessary to briefly detail the tactical ones that justified its creation as well. As stated by Micheal Reed in an e-mail that he sent the Tor-Talk mailing list in 2011:

> "[...]The original *QUESTION* posed that led to the invention of Onion Routing was, "Can we build a system that allows for bi-directional communications over the Internet where the source and destination cannot be determined by a mid-point?" The *PURPOSE* was for DoD / Intelligence usage (open source intelligence gathering, covering of forward deployed assets, whatever). Not helping dissidents in repressive countries. Not assisting criminals in covering their electronic tracks. Not helping bit-torrent users avoid MPAA/RIAA prosecution. Not giving a 10 year old a way to bypass an anti-porn filter. Of course, we knew those would be other

> unavoidable uses for the technology, but that was immaterial to the problem at hand we were trying to solve (and if those uses were going to give us more cover traffic to better hide what we wanted to use the network for, all the better...I once told a flag officer that much to his chagrin). I should know, I was the recipient of that question from David, and Paul was brought into the mix a few days later after I had sketched out a basic(flawed) design for the original Onion Routing. The short answer to your question of "Why would the government do this?" is because it is in the best interests of some parts of the government to have this capability...”[50].

The government needs anonymity. In several situations this condition can be crucial in order to properly operate, to accomplish a mission or to reach an objective. Actually, this concept was already explained long before 2011. For instance, Paul Syverson extensively articulated the matter during a National Science Foundation (NSF) conference he held in 2004[51]. As explained by the engineer, among the many tasks that Tor had been designed to perform, there was also that of carrying out open source intelligence (OSINT) operations on the Internet. Resorting to a governmental network for monitoring a public forum or a website would basically nullify any law enforcement surveillance capability: indeed, a site administrator can easily track any request, identify any IPs and associate them to an entity (a public, commercial or institutional Internet Service Provider). Moreover, Tor can be employed as operational infrastructure for dynamic and semi-trusted international coalitions: as they are usually created ad hoc, in order to cope with a sudden emergency, the participants to these coalitions are often “partners in one crisis and adversaries in another, raising difficult security issues with respect to information sharing” (Philips, Demurjian and Ting 2002, 87). In this kind of exceptional situations OR can be an ideal solution for sharing a network with third parties without revealing the existence of the network itself or the amount of communication between all parties. Finally, Tor can be employed in other critical scenarios: among those mentioned we can have "politically sensitive negotiations" (i.e. when a government agent do not want to reveal his identity or, on the contrary, when a third party does not want to reveal his real identity to the government), "road warriors" (i.e. an undercover agent working in an hostile environment), "homeland security information to/from municipalities, industries", "anonymous tips (national security/congressional investigations)" and the deployment of an electronic vote system.

1.11. Onions and the academy

Among the elements that significantly influenced the history of Tor, as well as the form of the network and the criteria leading its evolution, there is the intensification of scientific debate about the development of online anonymous networks, which happened in conjunction with the mass adoption of the Internet in the '90s. The integration of Internet in commercial and civilian infrastructures, the advent of electronic commerce, the rise of the World Wide Web, its growing importance in the processes of social communication, the transition of this electronic medium towards an immensely wider and more diversified audience in comparison to that of the small community of scientists who had contributed to build it are factors that accelerated the pace of academic research about topics like anonymity, privacy and online security. According to Anonbib[52], a portal maintained by Roger Dingledine where the most relevant research papers concerning anonymous online communication are collected and selected, in the period ranging from 1977 and 1993 – year of release of Mosaic, a web browser universally being considered one of the most crucial software for the massification of the Internet – the papers regarding these themes were barely a dozen. In the period going from 1994 to 2004 (year of the Tor early public release), the research in this field grew exponentially until reaching the number of 176 publications. In 1996, when the NRL started to fund the first onion router prototype, Ross Anderson published a document where he defined the guidelines of the Eternity Service, an anti-censorship platform from which Dingledine drew inspiration for his work on Tor. In that same year Babel – a high-latency network conceived to make email communication anonymous – was released and Wei Dai launched his idea for the realization of PipeNet, a low-latency network whose concept is very close to that of Onion Routing. Crowds, Free Haven, MixMinion, Hordes, Herbivore and many other projects, for the most part funded by public universities, followed. As we will see in the following of the chapter, the history of Tor is situated within this scientific debate: indeed, its creators tirelessly worked in order to fill the gaps and solve issues that until then research had not been able to solve.

1.12. The founders

As we have seen, between 1995 and 2004 NRL and DARPA supported Tor development for a plurality of reasons, be them historical (namely, the importance of T/A in the military culture and in electronic warfare scenarios), strategical (the US national wealth, the well-being of its technological fabric and the emergence of a new epistemological war paradigm as the NCW) or tactical (that is, to conduct OSINT operations) ones. Yet, the reasons underlying the development of Tor are not exclusively limited to those just mentioned, nor they only pertain to a strategic vision being ascribable to some branches of the US army. Albeit in its early stage it had been funded by the US military apparatus, Tor was actually entirely realized by civilian engineers who were moved by very different motivations than those which have been analyzed so far. As Paul Syverson mentioned on the Tor-Talk mailing list in 2011[53]:

> "People seem to need a periodic refresher on this. I will just state the long public and published facts. Interpret them as you like. You can read more details at http://www.onion-router.net/History.html but here's a quick summary:
> I invented onion routing at NRL with David Goldschlag and Mike Reed in 1995-96 as a US Naval Research Laboratory project with initial funding from ONR. All of us were NRL employees at the time. Our first deployed system was in 1996 and source code for that system was distributed later that year. (Code was entirely US government work by US government employees, so not subject to copyright.) As part of a later NRL project, I created the version of onion routing that became known as Tor along with Roger Dingledine and Nick Mathewson starting in 2002. I have been an NRL employee throughout all this. Roger and Nick were contractors working on my project. NRL projects funded by ONR and DARPA were the only funding they had to work on Tor until 2004. The first publicly deployed Tor network was in 2003, which

> was also when the source code was made available and publicly licensed under the MIT license. The first funding Roger and Nick got to work on Tor that was other than as part of an NRL project was from the EFF starting in 2004. Tor got funding from a variety of sources after that, including several U.S. government projects, both before and since becoming a US 501 (c)(3) non-profit. You can find a summary at https://torproject.org/about/sponsors.html.en
>
> HTH,
>
> Paul"

Later in the chapter, I will explain which was the role played by the EFF in the history of Tor. In this section I aim instead to clarify another question – namely to understand the motivations that led Syverson, Dingledine and Mathewson to work on the OR protocol and to implement an infrastructure based on it.

1.13. Paul Syverson

Paul Syverson is an internationally renowned scholar with more than 200 publications and 16000 citations[54] to his credit in the field of epistemic and temporal logic, as well as anonymous communications. His interest towards OR was fueled by the will to find a practical solution to a logical problem that until the first half of the '90s appeared to be unsolvable, that is, to devise a communication protocol able to simultaneously provide Internet traffic anonymity and authentication. This problem is summarized in the research question that, as he personally stated in an interview released in 2015[55], takes the most of his time at the NRL, namely "How do you characterize information flow through a system when you have different levels that are all interconnected?". In other words, his work is aimed at keeping together in the same system information flows classified under different levels of secrecy (i.e. 'top secret', 'secret' and 'classified') without producing accidental leaks between them. More precisely, Syverson conceived and formalized a method of communication to be employed in a network like the Internet so that one can reveal her identity to a third party – a person or a system that must verify it for legitimate reasons, such as to authorize the access to data set – and conceal it from everybody else at the same time.

In plain words, the mathematician developed a protocol to keep together two aims apparently colliding one another, namely authentication and anonymity. In fact, authenticating with a system means to associate some credentials with an individual, so that she can access legitimately some data stored within it. On the contrary anonymity, Syverson claims, “is when there is a set of individuals and you can’t tell which of them did something". Anonymity wants to make harder (and possibly to delete) the possibility for an actor to understand who is talking to whom, while authentication is all about defining to whom a system can give access. How can these two things be held together? The relationship between anonymity and authentication is counter-intuitive. Syverson explains it in this way:

> "I might want to use Tor because I am logging in from a local area and I do not want somebody there to know that I am connecting up to NRL for whatever reason, but I am going to connect at my system at work. Well, of course I want to make sure that I am actually talking to my system at work, and I want them to make sure it is me. I do not want let somebody else into my account. We definitely want to authenticate each other. It is just that I do not want the network to automatically do that. That’s why in one of our paper even back in 1996 [...] we said something to the effect of ‘we created onion routing not so much to provide anonymity per se but to separate identification from routing’”.

In the above-mentioned example, when Syverson connects to his system at work he would produce a leak, namely a transfer of unnecessary information between different information flows being classified according to different levels of secrecy (the administrator of the local areafrom which he is connecting could easily discover the IP address to which he is connecting). As we will see in the next sections, Tor mitigates this problem because it deprives the network from the power to identify the origin and the destination of the packets in transit over it. Moreover, in Tor the end points of the infrastructure are directly tasked with traffic authentication. “And that”, Syverson claims, “fits a lot with the design of the Internet going back to the beginning where the network is about moving the bits around efficiently and it’s the hosts at the end that [should authenticate each other]”. A principle that he illustrates with an anthropomorphism:

> "This also fits, to some extent, the way I think… it is a sort of more similar to day to day life, it is kind of funny that people may think otherwise. I mean… If somebody show up at your door you might ask to some ID before you let them in, but you do not say: hold on, I am only going to let you in if you can tell me exactly where you started and the route you followed when you drove to get here’”.

Syverson’s idea of security recalls the spirit of the original Internet design to the extent that it is devised as a form of personal protection that everybody should be able to enjoy and practice in first person, without delegating it to third parties. On the other hand, this vision has been developed in a way that is perfectly compliant with the previously mentioned CHACS's research agenda goals. Indeed, OR is a protocol able to simultaneously guarantee all those properties which are necessary for the proper functioning of a HACS: security (anonymity and encryption make it complex to infer useful information from internet traffic, both with regard to its content and metadata), safety (the traffic authentication makes it more difficult to access protected systems without authorization), real time (Tor was conceived for low-latency protocols) and fault tolerance (Tor's distributed architecture guarantees the functioning of the network even in case of malfunctioning by one or more network components).

1.14. Nick Mathewson

During his academic career, Nicholas A. Mathewson developed research interests very similar with those of Syverson. When he was still a MIT student, Mathewson had worked on the development of several software designed to securely share sensitive information, by protecting their confidentiality at the same time. One of those is the Java Information Flow[56] (Jif), a Java-based privacy and security oriented programming language. In his master thesis (Mathewson 2000,2), Mathewson defined Jif as a language that can solve the following problem:

> "When people use untrusted computer programs, they would often like to give secrets information as inputs, but at the same time remain confident that unauthorized parties will not learn their secrets. Jif [...] enables them to have this confidence".

And (ibidem,6):

> "As people transmit more information of their electronically, they face two conflicting goals: they want to allow computers to process their confidential information, but at the same time they want to keep their information private. For example, consider an online tax-preparation service. The tax preparer's software needs to use financial records from the taxpayer and a proprietary database from the tax preparer, but the tax payers do not want anybody to learn more than is necessary about their financial affairs, whereas tax preparers do not want anyone to learn the results of their proprietary researches. However, both parties are forced to give their valuable information as input to a computer program".

For his master dissertation thesis Mathewson developed "a bytecode verifier that can check whether a piece of compiled Jif code is flow-safe" so that "users can be confident that the verifier will only approve programs that will not reveal their secrets without permission" (ibidem, 2).

Yet, his interest towards security and privacy is not only of technical nature. As he explained during a guest lecture that he held at the MIT in November 2014[57], the reasons that led him to dedicate his life to Tor are various. The first one was that of solving a problem – that is, the separation of routing and traffic identification – that as an engineer he found intellectually challenging. The second one was to create an open experimentation platform for other researchers interested in working on traffic analysis. Third, he wanted to run a social experiment: that is, he wanted to test on a mass scale the effects produced by a wide dissemination of encryption tools being specifically designed to ensure freedom of expression to people.

As told by Mathewson, OR

> “...on the engineering edge is a cool problem. It is an interesting project and nobody else was actually working on it. And my friend Roger got a contract to finish up a stalled research project before the grant expired. He did well and I said ‘hey, I join up’. After a while, we formed a non-profit and we released everything as open source”.

During his lecture at the MIT, Mathewson emphasized an organizational dimension of Tor which is not immediately evident to its user base: namely that since the very beginning the infrastructure was conceived as a research-oriented platform. Nowadays the study of anonymous communications turned to be 40 years-old but in the early 2000s, when Tor took its first steps, many important research questions about this topic were unsolved. This situation led the creators of Tor to build their platform, not only as a low-latency network for anonymous communications, but also as a "test-bed" for scientific investigation: an environment being designed in order to support research, to conduct experiments, to test hypotheses and to collect data.

> “a lot of these research problems [...] were not even close to being solved, so why do we start anyway instead of going straight into research? One of the reasons we thought that lot of them would not get solved unless there was a test bed to work on. And that's kind of been borne out because Tor has kind of become the research platform of choice for lot of works on low-latency anonymity systems and it has helped the field a lot in that way”.

In the long run this choice undoubtedly proved to be successful: indeed, the centrality and legitimacy of Tor in the field of academic research oriented to low-latency networks development is absolutely undisputed[58]. The benefits which resulted from it are remarkable. First, a dense network of relationships that the members of the project have intertwined with the major universities of the world. Second, a continuous debugging work by researchers looking for flaws and vulnerabilities in its code. Third, hundreds of scientific publications where possible network attack strategies (and techniques to mitigate them) are hypothesized and put into practice.

Nonetheless, Tor has not only been a scientific test-bed, but also a social one. So far, it has been the first (and the only) anonymous system for on-line communications to be implemented on a mass scale. This is something not to be taken for granted, if we consider that in the '90s the United States had been the theater of the so-called ‘Crypto War’, a political battle that pitted the hacker movement against some federal agencies (such as the NSA and the FBI), with these latter being determined to weaken encryption algorithms used for civilian purposes, so as to be able to crack them for investigative purposes (Levy 2002, 235-76). This clash was accompanied by a powerful media campaign being aimed at delegitimizing their use: at that time, many media outlets predicted a bleak future should encryption be adopted at a mass level. Mathewson describes this scenario and the role that Tor should have played in it:

> “…10 years in and a lot of big problems still aren't solved, so if we waited 10 years for everything to get fixed, we would have been waiting in vain. So, why do it then? Partially because we thought that having a system out there, would improve long term outcomes for the world. That is, it is really easy to argue that something that does not exist should be banned. Arguments against civilian use of cryptography were much easier to make in public in 1990 than they are today because there was almost no civilian use of strong cryptography then. And you could argue that if anything stronger than DES is legal, than civilization will collapse, criminals will never be caught, and organized crime will take over everything. But you could really argue that that was the inevitable consequence of cryptography in 2000, because cryptography had already been out there and it turned out not the end of the world. Further, it was harder to argue for cryptography ban in 2000 because there was a large constituency in favour of the use of cryptography. That is, if someone in 1985 says ‘let's ban strong cryptography’, well, banks are using strong cryptography so they'll ask for an exemption. But other than that, there weren't a lot of users of strong cryptography in the civilian space. But if someone in 2000 said, let's ban strong cryptography, that would be every Internet company. Everyone running an HTTPS page would start waving their hands and shouting about it. And nowadays strong

> cryptography bans are probably unfeasible although people keep bringing back the idea”.

Moreover, according to Mathewson, making encryption tools accessible to a very wide audience has very important consequences for society at large. In his perspective, anonymity is a positive value because it makes possible a better communication and understanding of the surrounding environment. It allows to speak more honestly, to get "better information around the world", and it makes people less inhibited by the possible social consequences of their actions. Anonymity favors the affirmation of a crucial principle, namely freedom of expression, which has to be guaranteed – not only politically, but also resorting to appropriate technological tools.

> “Humanity has a lot of problems that can only be solved through better and more dedicated communication, free expression, and more freedom of thought. I do not know how to solve these problems. All I think I can do is trying to make sure that all I see as inhibiting discussion, thought or speech, becomes harder to do”.

1.15. Roger Dingledine

Mathewson’s vision is shared by Roger Dingledine who over the years has proposed a much more comprehensive and elaborate version of it. Ever since he was a MIT student, Dingledine worked at the development of technical systems being devised in order to ensure that individuals could enjoy an absolute freedom of expression and access to information. The technologies conceived by Dingledine embody a mindset, a worldview, according to which the exercise of such freedoms must never be hindered by anybody for any reason: resorting to them or not is an exclusive prerogative of the individual that, in this specific field, is imagined as the sole arbiter of her own choices. In order for freedom of expression and information to be effectively safeguarded on a political level, it is not enough that they are protected by the rule of law: in addition to this, they must be materially translated, and thus technically implemented, in the layers of the Internet Protocol Suite.

Dingledine has tried to transfer this perspective into the technologies which he created, with the aim of reshaping the power relations characterizing the Internet in favor of the individual for many years now. His master thesis (Dingledine 2000) is an example of this approach. In the dissertation, he articulates the design and the technical implementation of Free Haven (FH), an infrastructure being aimed to enable the anonymous publication of sensitive documents on the Internet.

Started in December 1999 and later put on stand-by due to a set of design problems that would have prevented its real-life deployment, FH was created with two goals in mind: a) protecting the identity of those who wanted to make a document public b) preventing any form of censorship and ensuring the availability of such document to the public by hiding the geographical location of the server on which it was uploaded. As explained by Dingledine in the introduction of his thesis, these goals are contextual to the transformations that were affecting the Internet infrastructure at the end of the ‘90s. On the one hand – he says recalling Eric Raymond’s writings on the abundance of the open source ecosystem (2000b) –, in that period cyberspace was characterized by important technical advancements, such as an ever increasing bandwidth, a steady growth of computational power and a continuous increase of the amount of storage connected to the network. Yet, since the Internet was not designed to protect users' anonymity and data confidentiality, it could have easily become a powerful domain tool:

> “Governments and especially corporations are beginning to realize that they can leverage the Internet to provide detailed information about the interests and behaviors of existing or potential customers” (Dingledine 2000, 4).

Incidents such as the lawsuit against Johan Elsingus – administrator of the popular Finnish anonymous remailer Anon.penet.fi which he was forced to shut down in 1996, after the pressures made by the Church of Scientology – and the arrest in 2002 of the Norwegian hacker Jon Lech Johansen – guilty of disclosing a vulnerability in the Content Scramble System, used by the entertainment industry to encrypt DVD contents for licensing enforcement – were seen with concern by hackers. Mentioned in Dingledine’s thesis as well, these events were read as alarm bells signaling the possible advent of an authoritarian and conservative society, being favored by the presence of a technical infrastructure like the Internet. Indeed, since the web always made possible to trace back the identity of whoever expressed an opinion on-line, it could have become an unsafe environment to express uncomfortable, unpopular or unconventional ideas.

FH was a technical answer to this state of affairs, being elaborated in order to overcome the lack of an "adequate infrastructure for truly anonymous publications and distribution of documents and data". FH would have provided a secure communication tool "for a wide range of activist projects which uses the Internet for publicity but focus on helping real people in the world" (ibidem, 5). Among these:

> “Pirate Radio, a loose confederation of radio operators joined in the belief that ordinary citizens can regulate the airwaves more efficiently and more responsibly than a government organization; as well as mutual aid societies such as Food Not Bombs!, an organization which “serves free food in public places to dramatise the plight of homeless, the callousness of the system and our capacity to solve social problems through our own actions without government and capitalism” (ibidem, 5).

The examples mentioned by Dingledine are of great interest. The reference to Pirate Radio’s self-regulation practices and to Food Not Bombs! self-organization process seem to show the engineer’s distrust towards hierarchical, centralized and impersonal macro-institutions. Also, they are a sign of the trust he harbors for the intelligence of the individual and her ability to solve a problem by taking charge of it in first person.

> “By providing tools to enable safer and more reliable communications for organizations fighting for increased rights of individuals rather than nations or corporations, as well as strengthening the capabilities of political dissidents and other individuals to speak out anonymously about their situations, the members of the Free Haven Project hope to help to pave the way to a modern society where freedom of speech and information are integral parts of everyday life” (ibidem, 5).

“Integral" is the keyword to consider here. Dingledine’s idea is essentially to incorporate concepts such as privacy, security and anonymity into the standards that govern the life of the network, so that they can ensure freedom of speech and information by default.

Like Tor, FH aims to have a wide and systemic range, namely, to push "the world to a few more steps in the direction of free and open information and communication". A vision that is openly inspired by the Ross Anderson's paper "Eternity Service" (1997). The Eternity Service

> "includes a wonderful vision of how the world might work in the future in terms of data havens and distributed decentralized data storage [...] the overall goal is to build a system that provides highly available data: as Anderson phrases it 'the basic idea is to use redundancy and scattering techniques to replicate data across a large set of machines (such as the Internet) and add anonymity mechanism to drive up the cost of attacks'" (Dingledine 2000, 24).

FH is an attempt to modify, to hack the power relations structuring the network by evening them out in favor of the individual, and thus transforming the status of the users. In fact, FH aims to enable anyone, regardless of the resources at her disposal, to publish and to read documents without incurring in complaints or sanctions (be them social, legal or even moral). Even more importantly, this anonymous publishing system is designed to be content-neutral and to host any kind of material "without regard for the legal or moral issues for that data in any given jurisdictions" and without concerns "for its popularity or controversial nature" (ibidem 49). Indeed, the same users are called to assess the credibility and value of an information through a reputation system that FH includes. It is evident how an infrastructure of this nature embeds an enormous trust towards the individual and her capacity for self-determination. It is not up to the State, nor the market, nor the common morality or fashions to establish the legitimacy of a bit of information. On the contrary, it is the individual that has to reflect, document herself, debate and decide on a specific matter; however, in order to do so, she must always have access to the information that elicited a debate. In FH there is no authority, because ideally every individual (and therefore, ideally, every end point participating to the network) is herself an authority[59].

This design implies a trade off. FH is a system aimed to ensure information anonymity and persistence rather than its frequent query or a quick access to the published documents. Second, the infrastructure is voluntary-based ("we assume that there will be some generous individuals who believe in the goals of the system and will give some service" ibidem, 7): to be an authority, to govern herself, the individual must be personally involved in the management of the network, by investing time and resources in it. Third, a system like FH is content neutral and therefore can be effectively used for abusive purposes. Dingledine believes

> “that providing individuals with the power to speak in a free, persistent and untraceable manner is well worth the risk of that” (ibidem, 54).

Hence, infrastructures like FH or Tor were conceived as power equalizers. In 2014, Dingledine gave a brief interview for the NSF[60]. Asked to explain the reasons that led him to care about anonymity, privacy and security, he answered:

> “There are lot of people out there who do not have the level of power in the world that they should. So one of the features of Tor is that it levels the plain field so that you… for example, if you are working in McDonald's and you can't afford to have a different job but there are some sort of corruptions or something happening at your work place, you need a way to whistle the blow safely without getting fired for it. At every levels in the world there are examples of these things, so one of the great things about Tor is that it gives people power where otherwise they would not have it”.

In another interview released in 2006[61], Dingledine explained that Tor "is about the freedom of speech and is about all freedom of learning", while in an article published on the MIT Technology Review with the emblematic title "Dissent made safer"[62], he specified that it is the same individual who has to take charge of the protection of such freedoms, without delegating it to third parties. Yet, in order to do so, she has to be provided with adequate tools.

> “originally one of my big reason for working on Tor was to provide tools for people in the West – Americans and Europeans – to let them keep their information safe from corporations and other large organizations that generally aren’t very good at keeping it for themselves”.

As it emerges from this statement, Tor, at least in its early stage, was conceived with Western societies in mind, that is, contexts were freedom of access and information were already ensured by the rule of law: in other words, it has been essentially designed in order to be used by Western consumers or Internet users operating under a liberal jurisdiction. Dingledine emphasized this concept several times. For example in 2006, at the 23rd Chaos Communication Congress[63]; or in 2012 when, together with Mathewson, he was nominated by Foreign Politics[64] as one of the most influential "top 100 global thinkers" of the year. On both occasions, he made this statement:

> "We developed Tor originally with civil liberties in mind. We want to let people in free countries be able to communicate so that they can keep their freedoms".

1.16. Politics: defining the goals

Tor has been theorized and developed in order to reach several goals that a) reflect the motivations of those who created its code and the infrastructure upon which it is built; b) result from the historical contexts in which Tor has progressively established itself c) mirror cultural and political trends crossing such contexts. In other words, Tor cannot be simply classified as a technical system aimed to reach political objectives. Actually, it is also the technical extension of an articulated political system that made the creation of this technology possible. Let's try to summarize who are the actors belonging to this political system, the context they belong to and the goals they want to achieve.

1. Fixing one of the unintended consequences of the Internet and making T/A harder. This problem was initially faced by a military institution (NRL). This is no surprise, given the historical relevance of T/A in the military culture.
2. Advancing HACS research and creating prototypes to be later developed and deployed by the private industry, in order to increase the security of the US national technological infrastructure. This strategy has been defined in 1995 by the CHACS and it found its main motivation in the growing reliance of the US economic and social system on digital computer networks.

3. Creating communication protocols for Information Assurance. This goal emerges in the '90s with the rise of a new strategic military paradigm (NCW) which emphasizes information superiority as key element for dominating the battlefield. According to this doctrine, the army depends on the network whose availability hence must of be always assured, also under critical circumstances. The actor who supported this specific goal was another military institution (DARPA).
4. Creating and implementing a low-latency anonymity network in order to carry out OSINT operations on the Internet. This goal emerges contextually with the growing importance of the then nascent World Wide Web in social communication processes and it is shared by several US government agencies.
5. Making any forms of online surveillance, that harms freedom of expression and creates the premises for a conservative social environment, harder. This objective was pursued by hackers and academic researchers who interpreted the first Internet crackdowns as signs of an authoritarian involution of the cyberspace.
6. Developing an empirical research platform that could serve as scientific test-bed either to test the Tor infrastructure (its design, usability and deployment) and gain experience to answer unsolved research questions.
7. Deploying a low-latency anonymity network on mass-scale and making it a social test-bed, in order to evaluate the consequence of a wide adoption of encryption. This goal emerges contextually with the 90's 'Crypto War' and the attempt by several US federal agencies to delegitimize and discourage the usage of encryption protocols for civilian purposes.

1.17. Design: safety is in numbers and diversity

How did the community that built Tor make possible the achievement of these goals? In order to answer this question a) I will briefly illustrate what are the main conditions that affect the full functionality and the effectiveness of the infrastructure (that is to say, the diversity and the extension of the anonymity set and the network) b) I will explain how these conditions are met by four design criteria, namely usability, deployability, flexibility and simplicity[65] c) I will articulate how such design criteria are technically implemented in the network. The analyzed data have been mostly elicited from the Tor design paper published in 2004 (Dingledine at al 2004).

As we have just seen, there are two main goals Tor was built for. The first one is to create an experimental research-oriented platform in order to gain experience and answer unsolved research questions in the field of anonymous communications, as well as to evaluate the consequence of a wide social adoption of encryption. The second one is to create a distributed and T/A-resistant network running over the Internet (that is, an 'overlay network'). As previously mentioned, T/A effectiveness is inversely proportional to the amount of data an actor can gather and analyze: the more is the amount of traffic being intercepted, the more complex is the process to analyze it, the harder is to infer a meaning from it. Because of this reason, the capability of Tor to defeat (or at least to mitigate) T/A essentially depends on:

a) The extension and the diversity of the 'anonymity set' – that is, the number of participants to the network and the variety of the social groups they belong to.
b) The extension and diversity of the network itself – that is, the number of the network nodes (called 'relays'), as well as the diversity of the ISPs and the countries where relays are hosted.

The problem of the extension of the anonymity set is explicitly mentioned in the previously quoted Reed's mail. Indeed, since day one, the creators of OR were aware that an infrastructure based on it could have been used for a multiplicity of activities (like illegal file sharing, bypassing parental filters or covering criminal activities) that had nothing to do with the purpose for which it had been created for. Nevertheless, this dynamic was not seen as a problem: actually, within certain limits[66], it was a desirable effect that would have ensured a strong anonymity to the users. Indeed, the higher is the amount of traffic generated by those participating to the network, the greater is the difficulty for an adversary to analyze it and trace back it to its senders and recipients.

Yet, diversity and extension of the anonymity set are also pivotal elements to make Tor work as platform for scientific research and social experimentation. Indeed, a higher number of users does not only mean a stronger anonymity, but also the material possibility to test the network's functionalities and limits in real world, to observe how people use encryption for civilian purposes, to assess its impact both at technical and social level. Moreover, Tor's broad diffusion and public dimension can function as a magnet for the scientific community which would surely be more interested in working on an infrastructure being implemented on a mass level rather than on a laboratory prototype.

This applies for the diversity of the anonymity set as well: its use in different social contexts allows its wider experimentation and it is useful to identify the possible limits preventing its adoption. Yet, it has to be added that the heterogeneity of the anonymity set is not less crucial than its extension in order to ensure the effectiveness of the infrastructure. As explained by Roger Dingledine in an interview he released in 2009[67]:

> "It is not just safety in numbers, there is safety in variety [...] even if there were 100.000 FBI agents using Tor, you would know what is for: you are using the FBI anonymity systems. Even from the very beginning part of the work was to take all the others different groups out there who care about what Tor provides and put all them on the same network".

Hence, in order to make T/A harder Tor has to be used by an indistinct and large crowd – namely, one characterized by a wide range of interests, nationalities, language and technical skills, cultural backgrounds, genders, political leanings – whose participants cannot be associated with a homogeneous category, nor with a specific reason that led them to use the network.

Moreover, diversity is a crucial element to safeguard both the fault-tolerance and anonymity properties of the network. Indeed, if all the relays that made up the Tor network were hosted by a single ISP, its owner could easily observe the users' traffic and de-anonymize them. Furthermore, a single ISP represents a "single point of failure": it would be enough to take control of its infrastructure (or to deny the access to it) in order disrupt the communications of the Tor network. Similarly, if all the Tor relays were physically hosted in a single country, the local government would have the power to shut down the whole network in any moment by simply issuing a law or a court order that bans the use of Tor on its territory.

1.18. Debugging: testing the world for building it

Being anonymous on Tor is like experiencing a condition of anonymity within a crowd: the more people are part of it, the more it is likely to remain anonymous within it, by hiding among them. It could be said that the ontological condition of online anonymity provided by Tor is the following: in order for it to be useful for someone, it must be available and usable by anyone. Or, to put it differently, in order for someone to be able to exercise the power of being anonymous in a digital network, she has to share this power with everyone else who wants to exercise it. Because of this reason Tor was built with the principles of usability, flexibility, simplicity and deployability in mind (Dingledine et al, 2004). As we will see in chapter 5, more than 15 years after its initial public release, such criteria keep informing the developmental trajectory and politics of the infrastructure, while concepts such as usability and deployability are still at the center of a continuous discussion and re-modulation.

Deployability is crucial for Tor. As we have previously seen, the network must be operated by volunteers, eager to provide anonymity, bandwidth and computational power to the network. For this reason, it has been designed to be easily adaptable to the resources the operators can make available ("it must not be expensive to run [...] by requiring more bandwidth than volunteers are willing to provide" ibidem, 3) and deployable without requiring special efforts or technical knowledge (it must not be “difficult or expensive to implement [...] by requiring kernel patches, or separate proxies for every protocol" ibidem, 3).

Usability is a no less important for Tor (and for low-latency anonymity networks in general). Talking about it, Dingledine, Mathewson and Syverson write:

> “a hard-to-use system has few users – and because anonymity systems hide users among users, a system with few users provides less anonymity. Usability is not only a convenience: it is a security requirement” (ibidem, 3).

Tor must be easily usable by anyone: a software that is difficult to configure, that requires a specific technical knowledge, or that can be only run on specific operating systems, already embodies access barriers that make the number of users (and the amount of traffic they produce) smaller than it could actually be. In order to be useful for a US engineer specialized in computer security, Tor must be easily usable by a Brazilian professor, an Italian plumber or an Egyptian doctor. For this to happen, the software must be inter-operable ("we cannot require users to change their operating systems to be anonymous" ibidem, 4), it must have few configuration options and it must not produce prohibitive delays. Otherwise, it will be exclusively used by highly determined individuals (perhaps those ones willing to accept a slower network in order to carry out sensitive or highly risky online activities), being provided with language and technical skills (for instance, somebody who knows how to modify a configuration file by using a command line interface, or know how to use GNU/Linux or a *BSD operative system). Without an adequate usability of the infrastructure, the anonymity set is going to be small and homogeneous by default. Furthermore, usability blends together with deployability. Better deployability means more bandwidth, and thus a faster and more usable network, capable to attract many different types of users. However, as we will see in chapter 5, concepts like usability and deployability must be articulated in relation to social, cultural and political problems, which are obviously much more complex than choosing an operating system.

Yet, Tor was not only designed to be as much open as possible to users, but, also to scholars interested in online anonymity and privacy. The fact that Tor has been built from scratch with flexibility and simplicity in mind shows that its creators aimed to make it a research-oriented infrastructure. Indeed, in the Tor design paper flexibility is a feature described as necessary “so Tor can serve as a test-bed for future research” (ibidem, 4) and to investigate a set of problems shared by any other low-latency anonymity networks (for instance, certain types of attacks aimed at deanonymizing users). Moreover, the flexibility of the platform ensure that any hacks being conceived by other low-latency networks in order to resolve such problems could be implemented by Tor as well.

Also, Tor wants to be simple. More precisely, it aims to maintain a simple design in which only "the best accepted approaches to protecting anonymity" (ibidem, 4) are implemented, while those presenting critical issues are discarded. That is why its creators deliberately chose not to build a P2P system: this latter approach was defined “appealing” but with “many open problems” (ibidem, 4) that research had not been able to resolve until then[68]. It would have been useless to engage in the creation of such kind of system for daily use, knowing already that it would have presented hard-to-fix issues that could have made it unstable (and then, usable only by a tiny anonymity set). It would have made much more sense to work on an infrastructure in which such problems could have been tackled practically, perhaps by attracting other researchers interested in working on the development of solutions to be integrated into other infrastructures later. Moreover, Tor is not an infrastructure for protecting users from a ‘global passive adversary’, namely a hypothetical actor who can monitor the traffic in and out from an anonymous network and, by correlating its origin and destination through simple analysis techniques, de-anonymize the user who generated it. 15 years after the publication of the Tor design paper, the global passive adversary problem has still not been solved: if Dingledine, Mathewson and Syverson would not have accepted to create an "imperfect" system (namely, a system that can effectively mitigate some specific forms of T/A, but not all of them) Tor would have never been born and the research concerning anonymous networks would have never made progress.

In this sense Tor is an infrastructure characterized by an extremely pragmatic rationale. It aims neither to be perfect nor to solve any problems potentially affecting the networks for online anonymity. On the contrary, it aims to mitigate such problems by resorting to the best solutions available to its builders, though leaving opened the possibility to implement new ones in the future. For example, originally Tor did not aim to be a steganographic network (that is, it does not conceal the fact that somebody is connecting to the network) but, thanks to its simple and flexible design, it was able in 2006 to integrate new components in the infrastructure (bridges and pluggable transports) that perform this function.

If Tor was defined by its creators as “the second generation onion router”, it is exactly because its usability, deployability, flexibility and simplicity features[69] have made it usable “on the real-world Internet”. Unlike its predecessor, whose “only long-running implementation was a fragile proof-of-concept that ran on a single machine” (ibidem, 1), Tor is a system designed to be used on a large scale and in real situations, in order to reach a specific objective:

> “the original goal of Tor was to gain experience in deploying an anonymizing overlay network, and learn from having actual users. We are now at a point in design and development where we can start deploying a wider network. Once we have many actual users, we will doubtlessly be better able to evaluate some of our design decisions, including our robustness/latency trade-offs, our performance trade-offs (including cell size), our abuse-prevention mechanisms, and our overall usability” (ibidem, 15).

The fact that Tor is designed from the roots in order to be used on a daily basis is the feature that makes it an ideal platform of empirical experimentation. Its large-scale implementation allows to collect real data that involve real users, and to test the robustness of the network in real situations. The data being observed and gathered can be used in order to correct or modify any flaws or mistakes in its technical deployment. In turn, this allows to improve the platform and make its daily use easier. By testing the world Tor aims to constitute it.

1.19. Coding/1: distribute the trust...

What are then the technical properties characterizing Tor, and how these reflect the goals for which it was conceived, developed and funded? In the section of the Tor design paper entitled “Related Work” – basically a literature review summarizing the 20 priors years of research about online anonymity – the authors present a taxonomy of the different types of networks aimed at making T/A harder: they describe their properties, their flaws, as well as the trade-offs that such networks imply. It is worth to briefly summarize such categorization: even a general understanding of it is useful in order to understand the rationale behind Tor.

The first classification, introduced in 1981 with Chaum's Mix Net, differentiates between 'high-latency' and 'low-latency' networks. Tor is a low-latency network, whereas other anonymous infrastructures, such as the Mixmaster and Mixminion remailers – this latter being developed by Dingledine, Mathewson and Danezis (2003) –, are high-latency networks. Anonymous remailers are designed to make it harder for an external observer to understand who sent an email to whom. In order to reach this goal, they introduce high delays between the time of submission of a message and its delivery to the recipient (an email sent via an anonymous remailer can be delivered to the recipient even several hours after it has been sent). This approach increases the level of anonymity being provided but it is unsuitable for interactive communication protocols – such as HTTP for browsing the web, or SSH for accessing a remote host. However, high-latency networks enjoy an advantage over low-latency networks, that is, they are resistant to T/A being operated by the so-called, and previously mentioned, global passive adversaries.

The second major categorization proposed by Dingledine, Mathewson and Syverson differentiates between 'single-hop' and 'multi-hop' networks. Tor is a multi-hop network, whereas a Virtual Private Network (VPN) is a single-hop network. A VPN is an encrypted tunnel that acts as a proxy between a sender and a recipient and it hides the IP address of a client. This kind of network is essentially based on the concept of 'centralized trust'. Here, privacy protection is entirely delegated to the system owner and it depends on the policy that she adopts in order to manage it: indeed, she can always read the origin and the destination of the traffic routed through the VPN. Instead, multi-hop networks are based on the concept of 'distributed trust'. This concept has been defined only later (Dingledine and Mathewson 2006, 3) as follow:

> "an infrastructure made up of many independently controlled proxies that work together to make sure no transaction's privacy relies on any single proxy. With distributed-trust anonymity networks users build tunnels or circuits through a series of servers. They encrypt their traffic in multiple

> layers of encryption, and each server removes a single layer of encryption. No single server knows the entire path from user to the user's chosen destination. Therefore an attacker can't break the users anonymity by compromising or eavesdropping on any one server".

Also, distributed trust is the feature that makes Tor ideal in order to operate in non-optimal conditions. Indeed, its architecture "is distributed, fault-tolerant and under the control of multiple administrative domains, so that no single onion-router can bring down the network" (Goldshlag, Reed and Syverson 1999, 1).

Ultimately, there is a third problem reviewed by Dingledine, Mathewson and Syverson, that is to say "which protocol layer" a low-latency network must "anonymize" (Dingledine at al 2004, 3). A circuit-based multi-hop network can directly anonymize IP packets, or TCP streams or HTTP traffic requests. In turn, each of these choices presents advantages and disadvantages, as well as "a compromise between flexibility and anonymity" (ibidem, 3):

> "a system that understands HTTP can strip identifying information from requests, can take advantage of caching to limit the number of requests that leave the network, and can batch or encode requests to minimize the number of connections. On the other hand, an IP-level anonymizer can handle nearly any protocol, even ones unforeseen by its designers (though these systems require kernel-level modifications to some operating systems, and so are more complex and less portable). TCP-level anonymity networks like Tor present a middle approach: they are application neutral (so long as the application supports, or can be tunneled across, TCP), but by treating application connections as data streams rather than raw TCP packets, they avoid the inefficiencies of tunneling TCP over TCP" (ibidem, 3).

In the early versions of Tor, TCP packets were cleaned from identifying bits before being routed through the network. This function was performed by 'application proxies' created for the specific aim of stripping from the Internet traffic bits of information – such as a 'cookie' or a 'HTTP referrer' – that could be used to identify an individual. Yet, this approach to protocol cleaning was unpractical and extremely expensive because it required to write and to maintain an application proxy for each of the thousands TCP-based protocols[70] present in the Internet Protocol Suite. As stated in that same design paper, most of these application proxies “were never written, so many applications were never supported” (ibidem, 1). This issues threatened to significantly reduce the Tor deployability, as well as the possibility of using it in many daily situations. As a workaround, Dingledine, Mathewson and Syverson chose to design the system so that all the user’s traffic was sent towards the infrastructure only through a single TCP-based protocol, that is SOCKS. This choice allowed to delegate protocol cleaning functions to third-parties applications (such as the Privoxy software) and, thus, relieved the burden of developing dozens of proxy applications. Finally, the fact that Tor developers conceived the software in order for it to be run without any kernel modifications – a complex operation that would have reduced its portability and usability for non-expert users – is a clear sign of the focus they put on system deployability.

1.20. Coding/2: ...and distrust the infrastructure

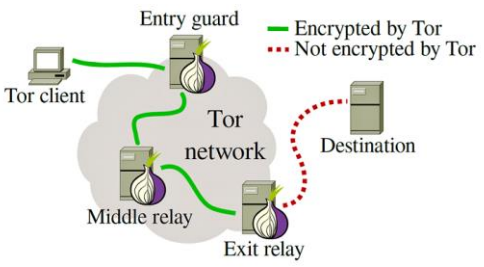

Fig. 10: How Tor works

Tor was designed for stripping the Internet infrastructure of a series of technical functions and reassigning their control – along with the power resulting from them – to users. More precisely such functions – for instance traffic identification, authentication or encryption – are object of a process of disintermediation, that is they are not being performed anymore by the infrastructure but are directly taken over by the clients connecting to it. In this section I will give a brief overview[71] of

a) the most important technical functions that in Tor are directly assigned to and performed by the clients

b) the transformation of the user’s status produced by this transfer of functions.

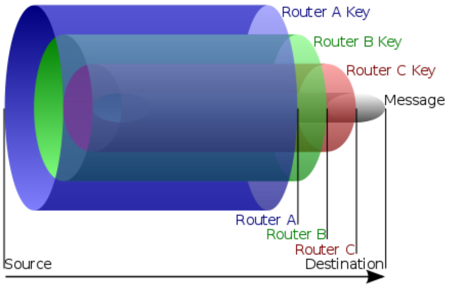

Fig. 11: Tor's telescopic path-building design

First thing first, Tor separates routing and identification of the traffic. Unlike what happens with the IP, Tor relays do not need to identify the origin and the destination of a datagram in order to transmit it from one network end to another. Only the sender of a data packet knows the whole path that its traffic follows in order to reach its destination. The network is conceived so that no actor – be it an internal one, such as a relay owner, or an external one, like an ISP observing the traffic flow – is in the position to identify who is talking to whom. It follows that when using the Tor network, a user is vested with a power which is denied by default on the Internet: in fact, she is anonymous either to the recipient of the datagram and to the very infrastructure carrying it over. Yet, nothing prevents her from associating her true identity with the traffic she generated, if she wish to (for instance by signing an email or by posting a blog with her real name). Importantly, a user can exercise this power on her own, without trusting anybody else but her personal device. On the contrary, when using a VPN, the power of being anonymous is not directly exercised by the user, but it is always granted by the system owner.

There are other Tor technical features that reveal how its creators aimed to empower its participants and deprive the infrastructure from as much power as possible. The first one is the “Perfect Forward Secrecy” (PFS), a function originally not included in Tor early releases[72]. PFS implementation aims to reduce the infrastructure to a mere carrier. In fact, when using PFS, a Tor client creates an encrypted tunnel using a “telescoping path-building design, where the initiator negotiates session keys with each successive hop in the circuit” (ibidem,1) Such keys are “ephemeral” and, once a session is over, they are deleted. Since the responsibility of negotiating an encrypted circuit completely falls on the shoulders of the client and not of the relay – which is nothing else that a dumb transit channel, unaware of the content and destination of the packets that it is routing and not in charge of any task in regards to user traffic (like encrypting it) –, this latter has no ability to record traffic and, at a later stage, to compromise the succeeding nodes in the circuit in order to attempt to decipher it.

Moreover, the implementation of two specific features[73] – that is traffic integrity check and network congestion control – proves that Tor was conceived in order to move intelligence towards the network edges. Prior to 2004, overlay networks were lacking a load balance system in order to cope with traffic 'bottlenecks' (and for this reason their performance was far from ideal in case of great amounts of data generated by a high number of user). Alternatively, they were built with an "internode control communication and global view of traffic" (ibidem, 2) that could be used to compromise clients' anonymity. In Tor this problem was solved through a decentralized and end-to-end control system that allows to check any traffic overloads and to maintain the client's anonymity. Similarly, Tor also introduced traffic integrity check in order to avoid any data manipulation attempt operated by a malicious relay for de-anonymizing a client. Integrity check is an end-to-end functionality as well: indeed it involves only the nodes situated at the borders of the network and not the intermediate relays.

Tor also features some properties designed to protect the voluntary nature of the network, which is at the core of the concept of distributed trust. In order for the infrastructure to be constituted by many relays being controlled by independent individuals and organizations – that is, in order for it to grow and to become as much diverse as possible –, those who want to take part to the network have the possibility to modulate their contribution and choose their level of involvement according to the resources at their disposal. This possibility is technically embodied in two Tor configuration options. The first one is 'rate limiting' that allows a relay operator to limit the amount of bandwidth she wants to donate to the Tor network. The second one is the 'exit policy', that is, the possibility for a relay to limit hosts and ports to which it can connect to. According to the exit policy that an operator adopts, she can choose to manage a 'middle node' (that will forward traffic only towards other Tor nodes), or an 'exit node' (that can connect to any other host being accessible on the Internet). An exit node can be configured in order to limit the ports it gives access to, thus becoming a 'reduced exit' (for example by denying connections on port 25, normally associated with mail service and therefore generally used in order to send spam). Nonetheless, exit policies do not entails any limitation in regard to the content being routed by the relays, regardless of their lawfulness. Actually, configuring an exit node so that it filters traffic is explicitly discouraged by the Tor community. As explained by Runa Sandvik, a former collaborator of Tor, at the DefCon21 conference held in Las Vegas in August 2013[74]:

> "If you are running an exit node to filter traffic, don't run an exit node at all. Running an exit node to filter content in general means… who are you to decide what people can watch or non watch on-line. We all agree that child pornography is bad. But what if we gave people the ability to actually decide what Tor users can and cannot visit through their exits node, and I decide watching videos of cat is bad, so suddenly I am censoring a number of Tor users, who wants to look at totally legitimate things? […] So we just decided that we should not decide what users can and cannot watch. It also means that we cannot be asked or forced by anyone to censor anything or give any type of information. We do not have anything, we do not control the network. Users do".

The infrastructure is not an authority: users are and they control it. They have the power to choose the information to which they want to have access, what to reveal about themselves, as well as what they want to make public and accessible. This latter function is carried out by onion services (or simply 'onions'), that make accessible a service (for instance a web server or an instant messaging platform) through a Tor circuit. Onions (an evolution of the FH project developed by Dingledine for his master thesis) are perhaps the technological component of the platform embodying at most the Tor's creators will to bestow the network clients of an absolute freedom of communication – such that it can be exercised without the need to ask any permission to third parties. An onion geographical location is hidden to everybody, except to its operator who, therefore, cannot easily be sanctioned by third parties for the contents she publishes or the services she provides. Furthermore, since an onion is not associated with an IP address, it cannot be affected by a traditional DDOS attack, nor its online presence is subordinated to the decisions taken by a technical body like the IANA. The same can be said for its domain name: indeed, this latter has not to be requested to a third party (like the ICANN or a registrar), but it is self-generated when an onion is created. Moreover, onions have self-authentication properties by default. Since an onion domain (as it could be the Facebook’s one www.facebookcorewwwi.onion or the BBC’s one www.bbcnewsv2vjtpsuy.onion) derives from an univocal encryption key to which only the owner has access, it is impossible for a malicious actor to create false domains to hijack users traffic towards a site she controls. When somebody connects to an onion domain, she will knows for sure that she is actually connecting to the site she wants to connect. In other words, onions provide traffic authentication, a property that, as we have previously seen, IP does not cover. Finally, the communication between client and server is end-to-end encrypted by default: this means that an onion owner does not have to request (and most of the times to buy) an encryption certificate from a ‘certificate authority’ (CA) in order to protect the confidentiality of the traffic her site serves.

Therefore, there are 4 fundamental freedom technically embodied in the Tor infrastructure:

1. The freedom to choose which information to access on the Internet.
2. The freedom to choose which information to publish on the Internet.
3. The freedom to choose which information to share and with whom.
4. The freedom to choose how to contribute to the network growth (this last freedom is also amplified by the fact that the Tor code is open source and allows anyone wanting it to partake in its process of development).

The network end points – be them clients, onions or relay operators – are the only arbiters of their own decisions and they cannot become arbiter of those made by other users. The infrastructure is conceived to be as dumb and oblivious as possible: it has not the power of identifying the people using it, nor the content of the traffic they generate, nor the metadata associated with such traffic. The network cannot manipulate datagrams, filter or censor them. No authorities, such as IANA, ICANN or a CA, can assign scarce resources (like an IP address) or decide whether an individual could be on the Internet or not. Since, as we have seen, end points are in charge of many fundamental network functionalities, a Tor-based infrastructure is basically deprived of any power if compared to an IP-based one.

There is an exception to this rule represented by the ‘Directory Servers’ (DS), that is a limited numbers of relays that are “more trusted than others”. Their task is to describe the network topography and provide it to the clients, so that they can connect to the network. DS compile the ‘consensus’, namely a document listing the relays belonging to the infrastructure and their properties: their typology (middle or exit), their exit policy, the bandwidth they make available, the platform they run on, their up-time and IP address. Once the “consensus” is approved and elaborated by DS (this process occurs on an hourly basis), they sign it with dedicated encryption keys and make it available to the public. When a client connects itself to the Tor network, as its first step it downloads the consensus validated by one of the DS and it uses it in order to create a circuit. DS have the power to exclude a relay from the network (by not including it in the consensus) whenever it behaves in ways that could undermine the network security and efficiency. For example, if a relay uses an obsolete Tor version being affected by known security holes which the Tor developers are not going to fix, then it is going to be excluded from the network. Or if a relay stops working because of an outage, DS exclude it from the “consensus” so that the clients would not try to use it anymore in order to build a circuit. DS can be defined as the only authorities of the Tor network, and actually their presence makes Tor a distributed yet semi-centralized infrastructure: if the consensus is not signed and published every hour, clients do not know the network topography and, therefore they are not able to connect to it. At the same time, DS' powers are very limited: they establish a form of authority that cannot interfere with the freedoms that the network ensure to the clients.

Technically speaking, Tor is nothing but a network built either for *being as much stupid as possible* and for *making the Internet stupid* as well. Indeed, on the one hand, Tor makes it harder to co-opt several Internet administrative functions and to use them as if they were intelligence devices of tools of domain. On the other, Tor itself is a dumb transit channel: many of the technical functions which on the Internet are usually performed by the infrastructure, in Tor are instead removed from it and they are directly performed by the users. In this way such functions cannot be co-opted by third parties for purposes other than those for which they were designed (as it happens instead for the IP). Control is given back to users, there is no network owner and within this environment there are only a few administrative entities vested with a reduced power. Another way of thinking it: Tor is a weak infrastructure built for being unaware of the users activities, so that it cannot interfere with such activities. It is a mean for evading the IP rules on the network layer of the Internet Protocol Suite, thus loosening the forms of authority that such rules institute.

However, from a political perspective this process of authority loosening produces 'loose' political values (I use this adjective as a synonym either of 'vague' and 'unconstrained'). Indeed, Tor is a tool for building a technical environment within which the agency and the diversity of the network clients/ends/edges are protected and enhanced. Yet, practices such as 'bypassing the IP rules' or 'safeguarding the agency and the diversity of network clients' are not indicating a specific political identity: as a matter of fact, they can be – and actually they are – shared by many diverse subjectivities who are moved by political visions, often very different to one another. Anarchists or libertarian communists can see in Tor a tool for organizing. Liberals can see it as a technology for protecting civil liberties. The DoD see Tor as a communication protocol for ensuring information assurance to troops on the ground. Activists living in south-east Asia can interpret OR as a bridge for circumventing censorship. In the third chapter I will explain how the US Department of State sees in the network a means to keep the Internet "open" (namely compliant either with the interests of the US companies and Washington power politics). And, as we will see in the next section, right-wing libertarians can see in this infrastructure the perfect environment for creating markets not compliant with state regulations.

1.21. Organizing: infrastructuring

The fact that Tor is built by its own users, it is deprived of any power and it is devoid of any form of authority which could limit the freedom of the clients, explains why the infrastructure drew the EFF's interest, as well as its economical support, in 2004. EFF was created in July 1990 by John Perry Barlow, John Gilmore and Mitch Kapor in order to protect civil liberties on the Internet. More specifically, the purpose of the organization is to protect "free speech, privacy, innovation, and consumer rights, all of which it considers under attack by legislation in the off-line legal arena despite considering cyberspace a completely separate space" (Nhan and Carroll 2012, 389). Barlow, Gilmore and Kapor were actually brought together by the idea that the Internet was an intrinsically egalitarian and autonomous space, not being subject to the same laws ruling the "real world". Driven by a scarce trust in the US political institutions and convinced that in Washington there was a substantial misunderstanding of the then nascent forms of online communication, the EFF founders saw with concern the early attempts by the federal authorities to regulate the web. The first one was the Communication Decency Act (CDA), a bill promoted by the first Clinton administration, with the goal of forbidding and punishing the distribution of pornography to children under 18 years. Interpreted as a dry run for a wider political maneuver finalized to a progressive reduction of online freedom of expression, CDA was subject to a strong opposition campaign led by EFF, which among its culminating moments had the publication of the most famous 'Declaration of the Independence of the Cyberspace'. Written by Barlow (1996) in Davos – where he was following the work of the World Economic Forum as deelegate –, this political manifesto emphasized the importance of the Internet as an environment freed from State interference, where "all may enter without privilege or prejudice accorded by race, economic power, military force or station of birth". It is worth noting that Barlow put many times on the display his fiercely anti-government positions about any policies regarding Internet regulation policies. In an interview released to the American Libraries Magazine in September 1996 (Chepsiuk 1996, 51), he defined the US government as "savagely anti-Internet" and he claimed that its efforts to establish its authority over the cyberspace were "doomed to failure". In the same interview, he asserted that Washington was transforming the country in "a totalitarian state faster than any place I've traveled to". Barlow defined himself as a conservative, a word to which he attributes a precise meaning: "let's solve our problem ourselves and not turn to some big incompetent known as government to solve our problems" (Albanese 2002, 43).

Barlow's loathing towards state institutions is shared with John Gilmore, another EFF founder. Fifth employee at Sun Microsystems and author of the saying "the net interprets censorship as damage and routes around it", Gilmore is famous for being one of the most important exponents of the cypherpunk culture born between the end of the ‘80s and the early ‘90s. Cypherpunk are representatives of a far-right ideology known as Libertarianism, that among its political and cultural cornerstones counts individualism, state-phobia and the cult of free market. Driven by an absolute tension towards individual freedom, libertarians tend to consider themselves anarchists, although their vision has nothing to do with the European socialist tradition. On the contrary, as explained by Timothy May (1994), one of the founders of the cypherpunk culture, such idea of anarchy is closer to Friedman and Von Hayek’s neo-liberal doctrine, that is, to a free-market ideology that promotes voluntary economic transitions and does not accept any form of external interference regulating them, including the governmental one. Libertarians profess an anarcho-capitalist creed: hierarchies, rules and elected bodies do not disappear at all from social organization processes, simply they are not under the control of elected local authorities. Importantly, cypherpunks claim that this form of social organization can be made possible by the development of digital encryption technologies, whose impact would undermine the power of traditional institutions, leading to their progressive obsolescence. In fact, their ambition was to create virtual regions being delimited by and built upon “cryptographic pipes and bricks”: a global interconnected environment where any transactions and information exchange would occur outside the control of the nation-states which, being deprived of their authority and of their very reason to exist, would have eventually collapsed. Such vision of the future was explained by Gilmore in 1991 when, during the meeting “Computer, Freedom and privacy”, he stated:

> “And if we could build a society were information is not gathered? [...] This is the society that I would like to build. I want to pledge with physics and mathematics, not through laws, things like the true privacy of personal data, the true freedom of trade, the true financial privacy and a reliable control of identity”(Gilmore, 1991).

In the eyes of EFF members and cypherpunks a network like Tor – being devoid of authority, in which encryption rules are the only laws one can resort to in order to protect her identity, privacy and freedom of expression – should have sounded like an ideal tool, the perfect "cryptographic brick" to build the future world made of technological self-sufficiency and political independence that they envisaged. And even if OR on its own was not enough in order to achieve this ambitious goal, it still stood as one of the prime and most effective tools for users' digital rights protection. When in 2004 DARPA and ONR's funding programs started to run out, the EFF decided to temporarily succeed the two government agencies and to bankroll Dingledine and Mathewson's work for one more year. The operation was made possible by the mediation offered by Shava Nerad, a historical figure of US digital activism, as well as founder and first executive director of the Tor Project INC non-profit organization. As she recounted[75]:

> "[EFF] stepped up and said 'We usually get money, but this project is too important. We'll give you funding for a year, but in that time you need to raise funds, and get self sufficient".

The EFF support to Tor was made public on December 21, 2004, with a press release signed by Chris Palmer, former Staff Technologist of the organization and participant in the mailing list cypherpunks.to[76]. In the statement, Tor was depicted as "a network-within-a-network" able to protect a multiplicity of subjects like "the average web surfer, [or] journalists for community sites like Indymedia, [or] people living under oppressive regimes" from T/A and its dangers. Among these latter, the EFF statement mentioned tariffs variations applied by e-commerce websites on a geographical basis, as well as physical threats to people at risk. More in general, Tor is presented as an empowering tool for Internet users since it is associated the possibility to "exercise their First Amendment right to free, anonymous speech on-line".

The money provided by EFF was employed to develop a Windows-compatible version of Tor, a required step in order to enhance the system usability, to expand its anonymity set, to increase the amount of network traffic and to strengthen its anonymity. However, this moment was a very delicate step of the Tor's history. As Shava Nerad recounted in the above mentioned interview, between 2004 and 2005 Dingledine and Mathewson failed to achieve financial self-sustainability. Indeed, in spite of their efforts and their attendance to many hacker conferences, once the financial support of EFF ended "they were strapped. Nick went to work for PGP in California, and Roger was consulting”. Only in 2006, thanks to Nerad's help, they would succeed in turning a small hacker crew into a non-profit organization involved in the development of a full-fledged infrastructure and reaching a long-term economic sustainability. By then, the experiment took off. After years of laboratory and fine tuning, Tor was becoming a public network looking out on the world, on that complex scenario where it could have been broadly tested.

1.22. Fixing bugs and building new worlds

Tor puts into question the contemporary paradigm of the hyper-centralized and surveilled Internet, whose design produces a uniformity of technical standards, aesthetics, architectures, ways of communication and, ultimately, of life. In this environment, users’ autonomous choices are replaced with prepackaged options being unilaterally established by algorithms and platforms owners. Moreover, within it transparency can be easily turned into a tool for imposing penalties against anyone who chooses to be not compliant with dominant social norms. All this has been made possible because of the extended process of cooptation of which the Internet has been subject: in other words, its infrastructure has been used for purposes other than those it was originally designed for. In this perspective the Internet has been re-worked into an intelligence tool for producing knowledge about the final user with the aim of manipulating her symbolic and perceptive structures. When being re-engineered according to these criteria, digital networks dis-empower the user because they make her an oblivious and unaware being. Indeed, the only form of memory which she has is the data storage provided by OTTs: the network knows everything about her and, often, it is the only means that she has in order to know something about the world and her very self. By updating and actualizing the values of the early Internet – an oblivious and stupid infrastructure where intelligence was situated at the ends of the network – Tor aims to create an opt-out mechanism to bypass the above mentioned power structure. It does so by developing and maintaining technologies that

- Embody and reproduce weaker forms of power and authority (the Tor infrastructure is unaware of the users and not the opposite).

- Allow users to bypass existing forms of power and authority (the Tor infrastructure makes the Internet stupid).
- Protect network clients’ agency and diversity.
- Require that network clients are diverse and that they act in first person in order for the infrastructure to be fully functional.

Tor is a project that I would define as ‘cross-eyed’, with an eye pointed towards the past and another to the future. Indeed, as I have explained in this chapter, OR is a large-scale experiment aimed at fixing some of the bugs that afflict the Internet's original design and make it insecure. At the heart of this project there is the idea of “making the Internet stupid again” by using an overlay network designed for depriving the underlying infrastructure of some crucial functions and transfer them to the clients. Tor has been thought in order to move power, responsibility and intelligence as much as possible to the edges of the network. The idea of “distributing the trust and distrusting the infrastructure” closely recalls the inner meaning which inspired the engineer community that gave life to Arpanet. Such meaning is often summarized in David Clark’s saying: “We reject kings, president and voting. We believe in consensus and running code”. This kind of emphasis on individual freedom and autonomy is self-evident in the design of the Tor network, which, in turn, has been conceived for being oblivious and stupid.

Yet, Tor is all but a project being nostalgic of the “good old days”. On the contrary, not only its gaze is fixed on the horizon, but its whole development has been shaped by a historical context affected by deep transformations and crossed by different visions about the future and the role digital infrastructures should play within it. In this respect, Tor is essentially a prototype: not only because it is an artifact fostering a process of scientific innovation for creating new potential forms of organization, markets, ways of relation, worlds, but also because it is built “in a way that constructs a partial alignment across the heterogeneous shop floors of industrial research and development on the one hand, and various site of work and technology on the other” (Suchman et al 2002, 167). For instance, CHACS' research agenda was aimed at developing technologies for safely turning US civilian, commercial and military infrastructures into digital networks: at that time, an urgent issue since the cyberspace advent was opening up the way either for new possibilities (like e-commerce) and risks (namely, the total dependence of the national economic fabric from the Internet). In turn, DARPA's funding had been provided with a similar rationale. Technological advancements had made possible the advent of NCW, a new strategic paradigm being characterized by alternative organizational forms of the army. However, these latter required long-term research efforts before being consistently employed on the ground. From their part, hackers like Syverson, Dingledine and Mathewson, had sensed how the promise of the Internet – that of a society built upon freedom of information, individual responsibility, self-management and control over the process of technological development – was shattering precisely while digital networks were becoming a mass technology. As a matter of fact, the creeping scenario that was taking shape resembled to a totalitarian nightmare made of conformism, repression and surveillance, which, perhaps, could have been rectified by an experimental use of encryption at a societal level. A vision that was shared by the cypherpunks who, however, saw in Tor even a leverage for shaping the anarcho-capitalist future being envisaged by Timothy May and Eric Hughes in their political writings.

Yet, as we will see in the next pages, the experimental dimension of Tor goes far beyond what has been explained so far. Between 2004 and 2017, this platform has been a magnet capable to attract a plurality of different people who, through their contributions, not only have imagined and have realized new practices and technologies to fuel the development of the infrastructure, but they have even highlighted its original conceptual limits and have proposed several solutions in order to overcome them. Moreover, with their tireless efforts, these pople have discovered new bugs – be them technical, political, cultural and organizational – affecting the FLOSS culture from which Tor originates and they have tried to fix them. Finally, the experience that they have gained in the field of anonymous communications have allowed them to affirm the complete inadequacy of the traditional concept of privacy: as we will see, the reflections which they have shared with me during the interviews overwhelmingly show the need to develop new practices and concepts that can cope with the urgent challenges and dangers that the era of mass surveillance holds for us.

These premises being made, I introduce my research questions:

1. What are the politics pursued by Tor in a condition in which the Internet has become fully undemocratic?
2. What are the structures of power and cultural imaginaries embodied into the Tor infrastructure?
3. How do Tor developers interpret the concept of privacy and translate it into the technological artifacts they build?

My goal is that of producing an analysis in order to explain which were the needs that led to the creation of this anonymous communication network and to interpret them in the light of the historical context within which they occurred. Moreover, my work seeks to clarify how the presence of Tor in the current Internet ecosystem produces a reconfiguration of specific power relations, within and outside the web.

2. Methodological approach to infrastructure

2.1. The problem of infrastructure: a relational concept

As explained in the previous chapter, the aim of my research is to understand what are the power structures and the imaginaries characterizing Tor. In other words, my goal is that of producing an analysis in order to explain the reasons behind the creation of this anonymous communication network and to interpret them in the light of the historical context within which they occurred. Moreover, my work seeks to clarify how the presence of this infrastructure in the current Internet ecosystem produces a reconfiguration of the power relations which it embodies.

But what is exactly an infrastructure and how can we study it? This word is usually associated with the idea of a technological network built for supplying and exchanging services and commodities over space. For instance, according to the definition provided by the Oxford Dictionary, infrastructures are “the basic physical and organizational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise”. Similarly, the Collins’ refers to them as “the basic facilities such as transport, communications, power supplies, and buildings, which enable” the function of a country, a society or an organization. Also, Treccani’s encyclopedia describes them as “structures or set of elements which form the basis of other structures” or “the complex of facilities and installations needed for operation of rail services, airports, etc.”. All the aforementioned definitions assume infrastructure as a “built object” and they are characterized by a strong emphasis on the physical layer underlying its technical functionalities.

Although not being incorrect, this approach presents some relevant limits, because it ignores some important ontological peculiarities that pertain to this subject matter. Although thinking about an infrastructure exclusively as an artifact allows to answer a certain number of questions concerning its operational dimension – for instance how has it been built? How does it work? What are its technical features? How can they be changed in order to achieve greater efficiency? – such perspective proves to be unsuitable in order to bring to the light its political rationality being built into the very fabric of the technical work (Neumann and Star 1996), as well as the material consequences that it has on the political processes. As a matter of fact, the political character of the infrastructure cannot be explained just with a mere description of the basic elements of which it is made of. On the contrary, they must be adequately interpreted in the light of the historical context within which they are situated and that they contribute to transform. In other words, the problem of the infrastructure is not so much the *what* but the *when:* as claimed by Star and Rulheder (1996, 113) "infrastructure is a fundamentally relational concept" since a technological network becomes infrastructure only in relation to the organized practices characterizing a given context.

2.2. A cluster of relations

There are many reasons why infrastructure is a relational concept. The first one is that it is always the result of an agreement, and therefore of a negotiation, between the different players who take part in its construction. Indeed, the configuration of the infrastructure itself and the minimal choices related to its implementation – for instance the standards and protocols it is based on, the kind of services it provides or the shape of its architecture – tend to favor the rise of specific social values, needs, beliefs, desires and identities, at the expense of other ones (Edwards 2003; Burrel and Dale 2003): as such, they are the objects of a heated dispute between many different actors who are driven by heterogeneous interests. The rise of political tensions around an infrastructure is a phenomenon that inevitably comes along with its evolution and development. Indeed, as we have seen in the first chapter, an infrastructure is a network which provides resources and services: however, these are usually distributed in an uneven manner, such to be reason of discrepancies, different ways of conceiving it and conflicts on different scales (Star 1999). This happens because for any problem the infrastructure is called to solve a certain number of possible solutions always exist, each of them implying a specific combination of techniques, practices, resources and organizational forms. An information network can be based on a client-server architecture or on a peer-to-peer one. An electrical grid can be powered by a wind turbine system or by a nuclear reactor. A healthcare system can be organized on a regional basis or it can be ruled by the federal government. Adopting one of these solutions at the expense of another is not a trivial choice, since not only each of them is produced by a power relation but, in turn, produces power relations. As a matter of fact, each configuration of the infrastructure corresponds to a configuration of power that affects the life of the different subjects exposed to the existence of the infrastructure in an uneven manner: different distributions of socio-technical solutions match different distributions of opportunities, possibilities, benefits and justice which transform that stakeholders' status (that is, their quality of life, their working experience, the right and the privileges that they enjoy) (Jackson et al. 2007). In this perspective, new infrastructures entail new "rules of the game" and, along with them, the establishment of new assemblages of power, authority, hierarchy and freedom that affect a large number of players, transforming both their individual conditions and their mutual relations (Bowker at al. 2010).

Since the concept of power is closely tied to that of infrastructure, the latter must never be studied in an abstract way, but always in relation to its spatial and temporal evolution. A complex socio-technical system is essentially the result of the historical context within which it is produced (Feenberg 1999, 155-223). As such, infrastructure has the tendency to transform itself in a relatively slow way, and therefore it has to be observed with the sense of time belonging to historians. Moreover, the political, social and ethical choices driving its development are borrowed from the "historical epoch" within which it is situated. With the expression "historical epoch" I refer to three different concepts outlined by Bowker (1996, 49-50). First, the ideas – to be conceived either as philosophical paradigms and epistemological assumptions – which in a given moment led to the growth of the infrastructure, affected its organizational practices and marked the steps and the pace of its development. Second, the history of the political and technological context in which it has seen the light. Third, the story of the actors who silently contributed to its construction behind the scenes. Using Virilio's words (1994, 14), we could say that the organization of an infrastructure always goes hand in hand with the manifestations of time. It is the place where mundane practices, great visions of the future and traces of the past converge and end up intersecting with each other. A proper infrastructural analysis requires to be simultaneously developed resorting to three different spatial-temporal interpretation grids, each of them being characterized by a specific scale (Edwards 2003, 191-204). A macro-scale perspective allows to examine systems and structures lasting decades and strongly affecting the development of an infrastructure (like the political economy of an organization, the strategic-military dimension of a historical period, the predominant political regimes or the cultures they express). A meso-scale analysis, instead, concerns the existence of institutions covering a shorter temporal duration (usually a decade) as it can be a corporation, an executive branch or a social movement. Finally, micro-scale is about individuals and small work groups active in a shorter time period (less than a decade).

Another relational character of the infrastructure is its reliance on other infrastructures. Indeed, as stated by Star (1999, 381-82), infrastructure is always sunk in other structures, social arrangements and technologies; it is build on the top of an installed base (and thus inherits strengths and limitations from it); it embody standards and protocols being developed by third parties. Moreover, when an infrastructure becomes crucial for the organization of a society – because it answers widespread social needs or creates them – it becomes a pivotal element for the existence of other infrastructures. When this happens, its study becomes possibly more complex: the more an infrastructure is affordable, the more it tends to be taken for granted and, therefore, to disappear. When it grows boundlessly almost embedding itself in the natural landscape and its use becomes daily routine, infrastructure becomes nearly invisible (Bowker and Star 1999). Because of all these reasons, it has to be framed as part of a human organization, as a relational property and not as a thing stripped of use (Star and Ruhleder 1996, 113).

Within an infrastructure, technique, culture, politics, ethics, organization and history coexist and mutually build each other. Because of this reason, it has to be imagined as "tangle to be unraveled". The research focus needs to be put on the stories and ideas of institutions and people who worked to the creation of an infrastructure; on the subjective experiences that contributed to its growth; on the different political, legal, socio-economic and technological contexts within which they took shape. Hence, the investigation of an infrastructure always requires a multidisciplinary approach since "when dealing with infrastructure we need to look at the whole array of organizational forms, practices and institutions that accompany make possible and inflect the development of a new technology" (Bowker at al. 2010, 103) and that converge in strategies able to involve the highest number of players (Edwards et al. 2007, II).

Since the aim of my research is to unveil the power structures, the imaginaries and the policies being embedded within Tor, I chose to adopt a methodological approach aimed at uncovering the complex cluster of relations that make this anonymous communications infrastructure possible in a scenario in which the Internet is increasingly characterized by undemocratic pushes and formidable power imbalances.

2.3. Method: ethnography of the infrastructure

Given the nature of my subject matter and the research questions I aim to answer, I have decided to investigate Tor with an infrastructural ethnographic approach (Star 1999; Star 2002). The ethnography of infrastructure is a way for seeing social order through 'boring things'. This research method aims to 'uncover' infrastructure and to show the human, political and interactive dimensions which are deeply integrated in its material aspects (such as protocols, technical specs, standards, plugs, wires, hardware, software). Albeit being extraordinarily unexciting and barely noticeable, these mundane elements are the crucial underpinnings of human activity and, as such, their analysis reveals "essential aspects of distributional justice and planning power" (Star 1999, 379). Indeed, artifacts and classifications are invisible mediators of action that embody "moral and aesthetic choices that in turn craft people's identities, aspirations, and dignity" (Bowker and Star 2000, 148). In order to make them visible and to decipher the representation of the world that they enshrine, it is necessary to strictly follow some general methodological tenets.

As previously mentioned, infrastructure is always sunk in other structures, be them social or technological ones: breaking up its sub-components allows to analyze their different physical and pragmatic properties, the tasks they support and the way they affect human organization. Moreover, an accurate analysis of the infrastructure requires to identify the conventions of practice that shape its form and functions. At the same time, it is necessary to keep into due account the properties of the installed base upon which the infrastructure is built, since the latter inherits strength and limitations from that base. Also changes and transformations investing the infrastructure are a fertile ground for analysis: given their modular nature, they are never simply imposed from above but they are the result of continuous negotiations whose study reveals the identity of the actors taking part in them and the terms of the relation unfolding among them. Finally, since infrastructure is learnt as part of a membership, it is fundamental to interact and become familiar with the artifacts that make it. Indeed, this is essential in order not to overlook or to miss some of its aspects which otherwise could be taken as natural (and therefore be uncritically accepted).

The ethnography of infrastructure is focused on the examination of the “decisions about encoding and standardizing, tinkering and tailoring activities”, as well as on “observation and deconstruction of decisions carried into infrastructural forms” (Star 1999, 382). It entails a multi-disciplinary fieldwork based on a combination of traditional tools such as interviews, observation, historical analysis, documentary analysis, biographical analysis, thematic qualitative analysis. Data can be drawn from many sources like design documents, technical specifications, manuals, changelogs, software repositories, newsletters, mailing lists, newspaper archives, financial reports or public meetings. The analysis of these data reveals the values and the ethical principles inscribed into the design choices that lead the development of an infrastructure. Also, it allows to understand the way the actors involved in its management conceive themselves and, finally, it highlights the historical changes happening around a technological network and affecting its formation.

Star suggests some “tricks of the trade”, “helpful for ‘reading infrastructure’ and unfreezing some of its features” (1999, 384), thus surfacing “the deeper social structures embedded in this tool" and dis-embedding "the narratives it contains and the behind-the-scene decisions" characterizing it (Star 2002, 110). Among these, it is possible to mention: the analysis of rhetorical devices through which the infrastructure's master narrative is built; the analysis of the infrastructural artifacts' metadata (which recount how knowledge is built and preserved); the study of the polysemy of these tools (that is, the different meaning they assume for both the actors involved in the creation of the infrastructure, and those excluded from using it); the investigation of the paradoxes of the infrastructure (namely of the small obstacles preventing its usage on a wider scale).

My research took inspiration from the work of historians, theorists and technologists who have shown how the emergence of political values in given historical moments led to the creation of particular technologies; and how, in turn, such technologies shaped well defined configurations of power. Eden Medina (2011) investigated the intersecting political and technological visions brought into the Cybersyn Project – a network built in Chile during the Allende government with the aim of collecting real time data about industrial production and advancing the peaceful fulfillment of a socialist regime – by engineers, trade unionist and political leaders. Laura DeNardis (2009; 2014) analyzed the Internet infrastructure under the lens of governance, thus showing how technical standards and protocols are political and have public implications: indeed, they are fields of tension over competing political and economic agendas being pursued by a set of heterogeneous global actors. Robert Ghel's (2014;2018) ethnographic explorations of Freenet, I2P and Tor were successful attempts to trace the historical conditions in which such networks found themselves and how they tried to overcome it. Chris Kelty's (2008) work about Free Software and the concept of "recursive public" – that is, a Public being "vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public" (ibidem, 3) – provided me with much inspiration for framing infrastructure as tool for reorientation of knowledge and power.

2.4. Ethnography of an open source infrastructure

Before moving to describe the research design, it is important to stress a few ontological peculiarities typical of the Tor network that affected – both positively and negatively – the research process. Particularly, the open source nature of the infrastructure and the informative transparency characterizing it proved to play an ambiguous role during the fieldwork. Indeed, during the past 25 years, the Tor community recorded and archived the whole history of the infrastructure in huge on-line databases. The abundance of such information made the work of reconstructing their meaning more complex, as much as elaborating a single coherent narration about them.

In spite of being a network created to "provide privacy to every human being on the planet Earth", Tor is not a secret society. On the contrary, the philosophy regulating its organizational forms is inspired by and borrowed from the FLOSS movement (acronym of "Free, Libre and Open Source Software") whose culture sees transparency as paramount. Indeed, FLOSS geeks consider this value as a cornerstone either in software development processes and self-government of the communities in charge of it. Nowadays, software source availability and modifiability has a meaning which "extends far beyond the arcane and detailed technical practices of software programmers and geeks" (Kelty 2008, 2): as a matter of fact, in the last forty years FLOSS has engendered "a unique combination of more familiar practices, that range from creating and policing intellectual property to arguing about the meaning of "openness" to organizing and coordinating people and machines across locales and time zones" (ibidem, 3). According to Weber (2004, vii), "by experimenting with fundamental notions of what constituted property" FLOSS communities have "reframed and recast some of the most basic problems of governance".

Tor is a FLOSS community, because its main feature is that of "adopting working methods that are open to the collaboration of all participants, meaning that it will potentially accept spontaneous input and interaction from any party that is involved in the creation of digital artifacts, be it a coder, a programmer, or even an ordinary user" (Ippolita 2007, 51). In other words, Tor is expression of an idea of Open Society which "is meant to consist of an 'open code' dispensation of which the possibility to provide input for improvement is freely available to all" (ibidem, 54). Because this can be possible, Tor, as many other open communities, keeps constant records both of its on-line and off-line activities – so that they can be consulted by those who would like to partake in its daily routine. As a matter of fact, the software code is public and accessible, and so are its design papers and its technical specifications.

Furthermore, in the Tor community the idea of openness is translated into many others organizational levels and the functioning of the infrastructure is based on an open source model of governance. Most of the mailing lists – which have been used by the community to share ideas, discuss issues and develop a heterogeneous planning ability – are public and archived online[1]. On the Tor wiki[2] it is possible to read the code of conduct drafted by the community members, the composition of the work teams responsible for the administration of different components of the network and even the transcripts of their public meetings (be them on the Internet or in real life). The bug tracker[3] hosts thousands of technical discussions occurred before and after the deployment of a new technical feature of the network. The Tor Project's software repositories[4], as well as those owned by its individual developers, are packed of technical and political considerations driving the infrastructure development roadmap. Even long-standing websites like www.onion-router.net or freehaven.net/anonbib are extraordinary archives (both being managed by prominent figures of Tor Project, like Roger Dingledine or Paul Syverson) providing historical and technical documents witnessing the evolution of the network. Interestingly, they can be even consulted with tools like The Way Back Machine[5], in order to visit their past snapshots and observe how such portals have changed across time. Also, in this way it is possible to browse and collect documentary materials which, for some reasons, are no longer accessible on the original website they were published. Moreover, the financial accounting of the project has been open sourced as well. Since 2007, the Tor Project has started to publish a yearly detailed audit of its financial situation, which is uploaded in a section of its official site[6] and reported with a post on the Tor Blog[7] homepage. Finally, Tor has managed to create Tor Metrics[8], a privacy-friendly statistical system designed in order to provide graphs and figures about the state of the network (users, relays, bridges, onion services, available bandwidth and much more) without putting users' anonymity in danger. Relay operators resort to these data in order to monitor the nodes they manage; the Tor Network Team[9] rely on Metrics data in order to assess the “vital parameters” of the infrastructure and orient future research and maintenance work; also, as stated by Bruce Schneier (an internationally renowned cryptographer formerly member of the Tor board of directors) Tor Metrics are political tools since they “are the ammunition that lets Tor and other security advocates argue for a more private and secure Internet from a position of data, rather than just dogma or perspective”[10].

Informative transparency has a recursive character: it is both a goal being pursued through a set of practices around which the existence of the infrastructure revolves, and an organizational condition which is necessary in order to get these implemented. Among its consequences, there is the production of a great number of data, signs, code and contents that seamlessly tell the past and the present of the network. Apparently, that is the dream of every researcher: an inexhaustible source of public information from which one could freely draw on. Actually the reality is quite different.

Indeed, the informative abundance of the infrastructure – an element shared by Tor with many open source projects – implies a number of disadvantages and backlashes that, if not adequately examined and tackled, threaten to undermine the outcome of the research. Particularly, the sources and the contents to analyze are so many that in the long run they can engender a sense of disorientation – ready to suddenly turn into real nausea – among those who try and sail through this *mare magnum* of information, and are continuously jostled all around the Tor ecosystem. In the next section I present my research design and I provide a general description of the path I followed in the attempt to navigate this data flow without being overwhelmed by it.

2.5. Research design

The sources which I drew upon during my research are the following:

1. Technical documents (Tor design papers, design papers of other anonymous systems of communication, manuals, conference proceedings, presentation slides, Internet Engineering Task Force’s Request For Comments).

2. Online archives of historical material pertaining development of Tor and anonymous communication networks (especially the www.onion-router.net and www.freehaven.net/anonbib websites).
3. Sitography of the Tor infrastructure (that is, online resources being used by the Tor Project participants for organizational goals, like its wiki, the bug tracker, its blog, the software repositories of Tor Project and of its members, the public mailing lists and Tor Metrics).
4. The Tor financial statements being published between 2007 and 2017.
5. Documents, political memorandums, financial statements of the US institutions funding Tor (among these being the Open Tech Fund, the Department of Human Rights and Labor, the Naval Research Laboratory, the Defense Advanced Research Project Agency) or that defined the strategical guidelines that led to its financing (State Department and White House).
6. Twenty open-ended interviews (involving either Tor developers, engineers, designers and hackers).
7. Observation of public hacker conferences participated by Tor community members (Italian Hackmeeting 2017, Chaos Communication Congress 2017, Internet Freedom Festival 2018).
8. Other open secondary data (public interviews released by Tor people, presentations or lessons footage held by the Tor community members, press releases, newspaper articles).

After having completed my literature review on the concepts of infrastructure, privacy, open source culture and internet governance, I started the ethnography (which took place from September 2016 to January 2019). I organized my empirical work into three phases.

In the first phase of my fieldwork (10 months), I decided to analyze some of the papers defining the foundational design of the Tor infrastructure. Moreover, I also analyzed several websites, archives of historical documents (like www.onion-router.net or www.freehave.net/anonbib), papers, slides and conference proceedings dating back to the second half of the '90s. Written by the creators of the OR protocol, these texts provide an extensive explanation about the reasons that led to its realization and the problem it wanted to solve. Design documents involve an ontological and epistemological way of thinking: they define the context within which a technology is situated, the problems that an infrastructure has to face and the possible scientific paradigms that can be employed in order to solve them. For instance, the original Tor Design paper (Dingledine et al. 2004) is a document answering questions like "what is an anonymous communication system in the present socio-technical environment?" or "which are supposed to be its features?" or "which are the most suitable approaches that can be employed in order to realize it?". Moreover, the authors provide an overview of the Tor architecture and design principles: they describe the aims the network has been built for (that is to say, to create a low-latency general-purpose anonymous communication system being resistant to traffic analysis attacks), its main features (practical, useful and anonymous), its threat model (that is to say the potential adversaries or the factors that could undermine the effectiveness of the network and de-anonymize its users), as well as its non-goals and limits. Furthermore, in these documents the security implications and the trade-offs of alternative anonymous and privacy-oriented network are analyzed. Going after the tracks that Tor hackers and designers left behind allowed me to get to the core of several problems concerning the political and organizational dimension of the infrastructure. Firstly, these electronic marks left on the Internet ground are a system of classification *per se* that, once questioned, were able to reveal the origins and the consequences of the organizational practices of the community. Secondly, by reading them I was able to identify an early set of players involved in the elaboration of such practices, along with the cultural and political context they belonged to. Thirdly, this information also allowed me to understand the values and interests embodied in the platform, underlying the phase of elaboration of a given technical process, in addition to their process of translation and implementation in a specific technological artifact. Fourthly, these data were fundamental for identifying the standards on which an infrastructure is built on, the social preconditions that make its existence possible, the relationship of dependency on which it is based, the ones it creates with other infrastructures and the way in which these are modified by the spatial or temporal reach of a network. After reading the Tor design papers, it was clear to me how the original aim of the network was essentially that of circumventing the rules characterizing the network layer of the Internet Protocol Suite. Because of this, I chose to analyze more in-depth the history of the IP, its political nature, its flaws, the way in which these can be politically used, the form of power that originates from its adoption and the kind of authority it establishes. With the goal of further investigating these topics – and to have a more complete picture of the technological context within which the creation of Tor takes place – I also consulted the several IETF's RFCs (including RFC 791, the original IP design document published in 1981).

In the second phase of my fieldwork (10 months) I carefully analyzed the Tor Project financial statements published between 2007 and 2015. Tor financial reports are basically bureaucratic documents called 'Form 990', also known as 'Return of Organization Exempt From Income Tax'. This document is a United States Internal Revenue Service form that provides the public with financial information about a non-profit organization. In this 80 pages-long report it is possible to find a huge amount of information about the economic management of Tor, like the name of its most paid employees, officers, directors, trustees and executives who belong to the organization; how the available resources were allocated; which were the most relevant items of expenditure; who the funders of the Tor Project are and the amount of its annual budget. These documents were read with the aim of figuring out who fueled the growth and the development of the infrastructure in the 2006-2016 decade and why. Funding is a matter of crucial importance since, as it happens for the great majority of open source systems, the political economy of Tor is poor and lacking of resources: without this financial support Tor would have never been the steady and influential organization it has become and, perhaps, like many other pro-anonymity networks that preceded it, it would not even exist. The analysis of these data (being it cross-referenced with the elaboration of an adequate theoretical knowledge – pertaining both to the role of the state in the processes of globalization and the meaning that the dissemination and spreading of electronic media have in US' foreign policy strategies) clearly showed who the macro-players involved in the definition of the infrastructure were, the historical context they came from, the political perspectives they stood for and how the Tor infrastructure would represent a negotiating and meeting ground for their different positions. These points have been analyzed further with an extensive research on the different US political institutions' websites (like the Naval Research Laboratory, the DARPA, the Open Tech Fund) that financially supported onion routing development through the years.

In the third phase of my work (10 months), I focused on the realization of twenty non-structured, open-ended interviews with members of the Tor community, each of them lasting between 60 and 180 minutes. I collected these data with the aim of building a patchwork of subjective experiences going along and integrating the analysis regarding to the historical, economic, political and technological macro-structures which shaped the infrastructure. Moreover, these interviews allowed me to understand that each interviewee produced her particular signification of the concept of privacy – a strongly contextual one, deriving from single individual experiences and specific political inclinations – and technically translated it into Tor technologies and infrastructure. My respondents were code developers belonging to the Tor Project, veteran relay operators, hackers creating software built on the top of Tor, representatives of associations supporting Tor, graphic designers and spokespersons. The interviews were almost completely made on-line and were preceded by an introductory phase during which I drafted a profile of the interviewee with information pertaining to her activity within Tor. In this perspective, the Tor wiki was a most valuable resource, since it allowed me to get beforehand a general understanding of the role of the interviewees within the community and to engage in extended, in-depth discussion with them at the time of the interview. I accurately avoided to ask for and conduct interviews during the hacker conferences I had the chance to attend. Hacker meetings can be considered the material condensation of everything being important to hackers (Coleman 2008) and they are spaces “that sustain the production and reach of virtual spaces and technologies” (Coleman 2010, 496). Because of this, I deemed it right to partake in these conventions with the spirit of a Tor user who is sincerely interested in the growth and management of the infrastructure, both for practical reasons (as I rely on it for most of my daily communication) and political ones (I deem OR as an equalizer of the power relations characterizing the Internet nowadays). I always tried to actively partake in the debates that I attended, in some cases also in order to test the validity of some ideas I was working on at that given time. This approach allowed me to sharpen my technical vocabulary and skills, to discover strengths and weaknesses of the infrastructure of which I was unaware, to get to know new projects being based on Tor, to meet people that maybe in a few months I would have interviewed and to become acquainted with some unspoken rules of the community. Among these latter, the one for which these meetings are sacred events, as they are one of those very rare occasions the community has for meeting and interacting outside the boundaries imposed by textual communication. In 2017 I had proof of that, briefly after the end of the relay operators meeting organized at the 34C3 in Leipzig. Faced with my request to have a chat, a famous Tor core member politely turned it down. Not because he was not interested in my research but rather, as he enthusiastically told me before dismissing me, because "relay operators are important!". Taking time out from their enjoyment, even deliberately ignoring that the participants often travel thousands of kilometers in order to attend them, is never a good premise for a successful interview (and it shows a substantial lack of regard for the sensibility of the interlocutor). When I was not able to directly interview the system builders of Tor, I resorted to several secondary data sources: past interviews, newspaper articles, press statements, videos of public events (like lectures or presentations).

Finally, I add that through each PhD year I learned to use and administrate a wide array of Tor-based technologies that, as I explain in the next section of the chapter, I extensively used in order to conduct my research.

2.6. Analysis

In the last ten months of the research I engaged with the analysis of the collected data. I carried out the analysis by using three different methods. The first one was the documentary analysis I resorted to in order to examine the Tor financial statements made public during the period going between 2006 and 2017. The examination of these documents proceeded step by step. Considering the amount of the data being taken into account (more than 1000 pages overall), at first I skimmed the reports being available with the goal of identifying their structural features and selecting the most relevant sections for my research purposes. After having identified the most significant budget items (particularly those pertaining to the incoming funding) I staggered them for each year, by splitting them in several sub-categories: amount (total and yearly one), kind of funding (milestone-based, deliverable-based or free), identity and nature of the funder (public or private actor), continuity of the funding over time, percentage donated by every single funder with respect to the overall balance. These data allowed me to cartography some fundamental aspects of the Tor political economy, like its degree of dependency from other actors, the interests they pursue but also the way this financing system affects the form, the functions and the daily management of the infrastructure. All these data were triangulated either with the literature review I produced in the beginning of my work on the topic (particularly with regard to the political economy of the open source projects and the digital diplomacy being pursued by the US State Department until the second half of the '80s) and other secondary data (like newspaper articles, financial reports or memorandums being published by the various organizations that secured sustainability for Tor in the medium term). The data being inferred from the financial reports also had a noticeable importance with regard to the interviews I conducted, because they suggested some questions which were discussed with my informants. This analysis work was collected in chapter 3, concerning the Tor's funding system.

The second method that I used is biographical narrative analysis (Rosenthal 2004). I resorted to this method in order to reconstruct the way Tor community members conceptualize the problem of privacy in regards to the infrastructure and the functions it performs. In general terms, the goal of this approach is to conceptualize how biographical experience, action logics and structure are interlinked to one another. Biographical narrative analysis involves the use of the open questioning to provoke narratives or reflections that allow the interviewee to explain her perspective on a given problem and the way she chooses to deal with it. The analysis of the semantics used by interviewees to narrate their own biographical actions allows to a) describe the way different people behave in different contexts in relation to a given problem b) identify a limited number of significant actions in relation to such problem c) reconstruct the way different actions and logic of action come together or are linked to specific context. The lack of a universally shared definition of the concept of privacy and the lack of homogeneity of the practices it is normally associated with (both issues are discussed in the introduction of chapter 4) convinced me of the need to adopt this method and to analyze the meaning of the concept of privacy in a situated manner, namely in relation to the biographies of my interviewees and to their subjective experiences within and outside the Tor community. For this reason, I chose to employ a particular interview style, encouraging the interviewees to describe their own idea of privacy in relation to their life experiences and to explain how it is translated and embodied in the management and development of the Tor infrastructural components they are in charge of. This kind of analysis also allowed me to bring into focus the historical and personal events that led the interviewees to contribute to Tor development. The analysis of these interviews, compared with a literature review concerning the many interpretations of the concept of privacy, underpins the structure of chapter 4.

Finally, the third method I used was qualitative thematic analysis. Through a comparison and a reading of collected data (interviews, Tor Project sitography, technical papers and newspaper articles) I reviewed the essential socio-technical conditions the Tor infrastructure is based on, and the technological policies being pursued by the community in order to ensure a reproducibility of the infrastructure. The close dialogue I had with the interviewees and their availability for debate were of great help to bring into focus the many limits affecting the infrastructure, that have been for many years subject to a tireless work of bug fixing, being it of technical, cultural or organizational kind. Following the suggestion provided by Star (1999, 383), during this stage of research I sharpened my ethnographic sensitivity as much as possible, by keeping in mind "that people make meanings based on their circumstances, and that these meanings would be inscribed into their judgments about the built information environment". This work has been merged into chapter 5 (Tor's technological politics).

2.7. Ethics

Conducting my research in an ethical manner has meant to autonomously build a research infrastructure. Its ethical dimension lies in the fact that its design was not prepackaged by third parties but it has been continuously conceptualized and modified in order to pursue three different goals. First, effectively fulfilling research data collection and retention; secondly, having a positive impact on the situation of my interviewees, mitigating every possible risk deriving from their participation in my work; and thirdly, defining clearly my positionality towards the Tor community. The infrastructure I am describing is based on two established hacker culture security models, namely ‘security by transparency’ (the technical infrastructure I used was completely based on FLOSS) and ‘security by compartmentalization’ (particularly I massively resorted to Qubes OS[11]). Also, it was entirely based on hardware being physically under my control, including the server where data were stored. These features made my research infrastructure either functional and ethical in regard to the purposes being listed above.

No data were gathered by resorting to closed-source software. The choice of adopting FLOSS as foundational element of my research infrastructure comes from the will of overcoming the security and ethical problems related with closed-source software. As a matter of fact, proprietary software is only released in binary form – namely, one readable by machines but not by human beings –, while its source code is not publicly available. As such, it is not possible to know how it works: without this kind of knowledge, there are no scientific evidences which allow a researcher to state that a specific software is suitable for safe management of sensitive data. On the contrary, relying on FLOSS allowed to partly overcome the aforementioned problem since the source code of the programs I employed is open and can be reviewed by whoever is interested.

It is worth noting that the source code openness is not a guarantee of security in itself. Because of this, I resorted to a second security model, namely security by compartmentalization. The foundational principle of this security model is grounded on the assumption that security measures, as much as they can be refined, always present flaws: therefore, rather than focusing on the protection of a whole system, it is much more useful to pursue a rationale of risk reduction. If a single target – in my case, a single laptop storing research data – is difficult to defend, it makes sense to turn and split it into multiple targets. This aim can be pursued through a technique called virtual isolation, consisting in the creation of a set of virtual machines (VM) that run within the computer's main operating system. A VM can be conceived as a computer within a computer. Any single VM can be dedicated to a different specific task: one can be used in order to store sensitive research data (like interview recordings and their transcription), one to write notes, one to surf the web, one to manage e-mail accounts, and so on. A configured set of VM provides an additional protection made of separate operative systems for managing alternate data without having to use multiple computers.

Before I started collecting data I got official ethics approval from the University of Leicester's ethics committee. Moreover, during my research, I followed the Research Code of Conduct and Ethics[12] that the university asks recipients of funding to comply. Finally, I have led the relationship with the interviewees by adopting the following practices. 1) In order to get in touch with them, I only relied on privacy-oriented e-mail providers. 2) Mails were daily downloaded and stored on my encrypted hard drive. 3) Whenever possible I carried out live, face-to-face interviews. Data were recorded on the external memory of the voice recorder, whereas internal memory had never been used. Once recorded, data were saved on a special partition of my laptop without web access, and wiped from the external memory of the recorder. 5) I adopted the same approach for phone interviews, even though I conducted the latter through Signal[13], a secure VOIP software. 6) I did not ask for, nor gathered any information on potentially incriminating subjects. In order to avoid my respondents said anything which could have harm them in a court of law, all my interviews were prefaced with this caveat and all the questions were structured with this tenet in mind. 7) No external transcribers were hired: I personally transcribed all the interviews and the recordings were destroyed at the end of my PhD. 8) Finally, my supervisors never had access to the raw audio recordings, nor to their transcriptions. In the “Appendix A” I provide a more extensive description of the minimum elements upon which my research infrastructure was built, the rationale behind their choice and the practices they supported.

3. The Tor’s funding system

3.1. Introduction

In this first empirical chapter I will focus my attention on the Tor funding system. More specifically, I will present and analyze the organization's public financial statements and the annual reports of one of the most important supporters of the project, namely the Open Tech Fund (OTF). By reading these documents I aim to identify a) the funders who financially contributed the development of the infrastructure b) the motivations and interests that lead them to support its growth c) the complex network of actors that took advantage from these funds d) the way these latter structured their relationship with the funders.

Tor's funding system has made the development of the infrastructure materially possible on a global scale, by ensuring the project a certain economic sustainability which, as we will see, open source projects rarely enjoy. The analysis of these data is therefore fundamental because it represents a good starting point for explaining the production mechanisms of the Tor network and the power relations shaping it. In addition, the onion routing funding system must be adequately taken into account because, as detailed in this chapter and the following ones, it has a decisive influence either on the organizational dynamics of the community and the on shape of the infrastructure itself. Finally, following the money is a great way to understand, not only the objectives pursued by the funders who support the network growth, but also the different historical contexts they belong to and, in turn, within which the infrastructure is situated.

3.2. Open Source: ethos, benefits and drawbacks

As mentioned in the previous chapters, Tor is an open source infrastructure. With the expression ‘open source’ I refer to two concepts overlapping one another. The first one is ‘open source software’, that is a computer program whose source code is released to the public domain under a license that makes it freely accessible, modifiable and distributable. The second one refers to a specific ‘scientific methodology’, namely a “team work method, grounded on meritocratic principles of excellence and based on a voluntary motivation and a precise ‘ethic’, combined with the will to enable everybody to access a resource, to use it, to modify it, and to distribute it without adding any further restrictions” (Ippolita 2005, 42). Although in the common lexicon ‘open source’ is usually associated with ‘free software’, these two concepts actually present relevant ethical differences. In fact, free software supporters claim that “a computer program must be considered as a math formula or a scientific discovery, namely a common good that everybody can study and improve according to her needs, as it is established by the four fundamental freedoms[1]” (Ippolita 2017, 182). In this perspective, sharing knowledge without restrictions is first and foremost a fundamental right provided with a strong moral value: indeed, “the core of the moral philosophy espoused by the FLOSS is a commitment to prevent limiting the freedom of others” (Coleman 2004, 509). On the contrary, open source enthusiasts consider the practice of sharing source code “simply as the best way to develop software” (Ippolita 2017, 182): they are open to collaboration with companies inclined to adopt such work method and, at the same time, they are willing to accept that a piece of software could be licensed on the market with some restrictions. Despite free software and open source are marked by such differences, in order to ensure an easier and more enjoyable reading hereinafter I will refer to both of them with the acronym FLOSS (acronym of “Free and Libre Open Source Software”).

FLOSS is generally considered superior and more convenient than closed source and proprietary alternatives: it is free (in the sense that everybody can freely take advantage from it), it is cheaper to build and to distribute (there is no need to paid fees in order to use it or to deploy it within a digital infrastructure), it is flexible to customize (a developer can copy and change a piece of software for her own purposes within the bounds granted by a license), it is easier to maintain and it is more secure (Eghbal 2016). In particular, this latter property is recapped by the popular adage “given enough eyeballs, all bugs are shallow” (Raymond 2000a). According to this precept, the very openness of source code is a security feature: indeed, the more are the users and developers involved in its audit and debugging process, the more are the chances to identify and fix any errors.

Security, stability, flexibility and maintainability of FLOSS result from an ethics of sharing which for coders is key to build "state-of-the-art computer programs, because it is precisely the ability to tinker, adapt and improve upon software that enables innovation to occur within software development" (Birkinbine 2020, 32). Indeed, openness makes it possible a recursive process of writing, deployment, refinement and rewriting of the code that results in its continuous improvement and it reduces the reasons to subvert it and to reinvent it (Kelty 2008). It is no surprise that since late 90's, many Silicon Valley companies have began to elaborate market strategies being aimed at co-opting open source practices in a corporate logic for increasing the quality of their products (Ippolita 2007; Deek and McHugh 2008; Birkinbine 2020). Actually, according to Tapscott and Williams (2008), FLOSS has been crucial to create economic competition in a market sector formerly ruled by Microsoft's feudal revenue system.

Yet it is worth emphasizing that the FLOSS sharing ethics had its roots and thrived in a very specific historical-cultural context, that is, the one emerged between the end of WWII and the early 80s in the US academic world. Universities and research centers like the MIT or Berkley were inhabited by a culture "which had no professional secrets, in which co-operative effort was the order of the day" and where "code was co-operatively written, freely shared and always regarded as being in the public domain" (Naughton 2000, 197). In this kind of environment, removing any barrier which blocked the access to scientific knowledge was paramount, an absolute moral imperative which ended up for being embedded even in Arpanet's original architecture: indeed, as noted by Barbrook (1998), its design implied the possibility of distributing information over multiple nodes of the network, thus assuming "intellectual property as technically and socially obsolete".

Nevertheless, it is important to remark that, besides being the result of an admirable idealistic ardor, FLOSS ethics had been made possible by solid material foundations as well, namely by an abundance of economic resources that the US scientific community had had the possibility to enjoy. In other words, if US scientists were in the position to donate their research findings to the public for free and “never bothered to incorporate intellectual property within the system” or to turn their work into marketable commodities, it was because “their wages were funded from taxation” (Barbrook ibidem). At that time engineers, researchers and hackers, not only had the opportunity to work in a relaxed environment and the chance to enjoy an almost absolute decision-making autonomy: above all, they were able to benefit from a boundless source of public funding allocated by the federal government (Formenti 2008). Indeed, in 1958, at the height of the struggle with the Soviet Union, the U.S. Department of Defense (DoD) founded the Defence Advanced Research Project Agency (DARPA) to achieve long-term technological supremacy. Responsible for the development of military technologies, DARPA financed thousands of projects, thus hoping that some of them would have ensured a strategic advantage over the enemy (Castells 2001). As also acknowledged by the protagonists of that extraordinary season – such as the engineers being employed at the legendary MIT Artificial Intelligence Lab, cradle of the Free Software movement in the 80’s – “ARPA money was the lifeblood for the very existence of hacking” (Levy 1994, 104) without which it would have never been possible to practice that radical ethics of sharing which is its main hallmark. In fact, with the end of the Vietnam war, when public funds allocated by DoD and DARPA began to dramatically decrease, laboratories, research centers and universities had to turn to the private sector which proved to be willing to grant the money as long as the research findings were protected by patents, copyright and non-disclosure agreements (Willams 2003).

The point is that FLOSS is a culture and an organizational method of work which originated in an unrepeatable historical juncture during which long term sustainability of scientific research was ensured by huge State funding being provided for geo-strategic reasons. Ethics of sharing and gift culture are elements which should not be interpreted only in a moral light: indeed, they are to be understood also as direct consequences of the abundance of material resources which characterized the context from which they arose. “Gift cultures” Raymond claimed in relation to open source economy “are adaptations not to scarcity but to abundance” (2000b). But what does it happen when open source method and ethics are transferred into a new context being characterized by conditions of scarcity, where neither the sustainability of scientific research nor the subsistence of scientists are guaranteed by taxes and public money? That is, in a context where the question to ask is no longer just "how to make a better science?" but also "how to pay for it?".

According to Eghbal (2016a), because of the lacking an adequate funding and wages system, FLOSS ecosystem has seen the rise of several critical issues which have called into question its celebrated ability to produce stable, safe and quality software. In the long term, permissive licenses, accessibility of the code, ethics of sharing, a culture against the privatization of knowledge and informal organizational structures have not been able to generate a sustainable business model. Big IT companies have shown little inclination in funding a non-rival asset like FLOSS, fearing that even their competitors would have benefited from it. Instead, individual users – who have been accustomed to get free access to software for years – have never worried about this problem, since they took for granted that somebody else would have taken care of it. Although it has become a crucial component of the global digital infrastructure, nobody pays for open source. Those who pay the price of this state of affairs are first and foremost FLOSS developers who see their physical and mental well-being, as well as the quality of their work, compromised.

The lack of resources and professional perspectives is a reason for burnout, stress and exhaustion which regularly turns into a loss of qualified workers. The low turnover and the limited staff available constitute an obstacle for code maintenance and audit with harmful consequences for its security. Finally, since FLOSS is lacking both a stable business model and steady revenues, only those who experience a privileged condition can work as open source developers: this results in an environment being affected by an important lack of diversity in terms of class, gender and race. In addition, FLOSS ecosystem is characterized by conditions of precarity, uncertainty and ultra-work due to the few funding sources available to its developers. Indeed, strategies such as crowdfunding, grants or consultancy for private companies ensure only a limited income over time. In addition, they require the acquisition of new job skills – such as learning to coordinate a fundraising campaign or creating a legal entity in order to apply for a public grant – and the waste of additional physical and mental energies. With a very apt comparison, Eghbal (2016b) defines this kind of livelihood nothing but a "lemonade stand". Zhu (2019) claims that "the state of how you make money in open source is getting tips", an activity that he defines far more tiring and frustrating than writing code. Saltz (2019) analyzed 58 popular FLOSS project and found out that most of them "are actually receiving income below industry standards and even below poverty threshold": his conclusion is that there is "a severe imbalance between work quality and compensation". In short, nowadays FLOSS ecosystem is very much different from the geek paradises – being defined by those who experienced them as "unique and ephemeral" worlds (Williams 2003, 73) – where it was born along with "gift culture". On the contrary, its production, distribution and consumption mechanisms are defined by power relations that, as claimed by Terranova (2000), make it a form of unpaid labor dependent on capitalist structures.

3.3. A transparent and semi-centralized funding system

Open source has a contentious relationship with money. And Tor? Has the project managed to achieve economic sustainability over the past 15 years? If yes, how? What is its annual budget? What are its main sources of income? What is the funding model it has adopted? How does such funding model affect its organization? As detailed in the methodological chapter, in order to answer these questions I have analyzed the Tor's financial statements[2] published between 2007 and 2015 and the OTF's annual reports[3] published between 2012 and 2018. This latter is perhaps the most important funder of Tor and, more in general, of many FLOSS communities who are committed in the development of encryption and censorship-circumvention technologies. In the next pages (sections 3.3 and 3.4) I will exclusively focus on the Tor' financial statements, while in the continuation of the chapter (sections 3.5 and 3.6) I will explore in depth the importance of OTF as a public incubator of privacy and security oriented technologies. A caveat before starting: the data being presented in sections 3.3 and 3.4 exclusively refer to the funds raised and managed by the Tor Project INC (TPI): others organizations affiliated with the Tor Project – whose members I have interviewed for this thesis, such as Guardian Project, Open Observatory Network Initiative (OONI), Globaleaks, Tails (that is, The Amnesic Incognito Live System) or Tor Servers – have their own separate sources of income.

TPI is a very articulated non-governmental organization (NGO) responsible for the development of the Tor protocol, the Tor Browser Bundle (TBB) and dozens of other tools being employed to administrate the infrastructure and to monitor its state. Also, TPI is appointed with other important technical and organizational tasks, such as studying users experience (UX), managing Tor Project's site and social media, creating contents for the Tor Blog, providing legal and technical support to users and relay operators, writing grant applications and organizing fundraising campaigns, just to name a few. From 2007 the number of people being hired by the organization has gradually increased, reaching 35 members among contractors, consultants, full-time and part-time collaborators in 2020[4].

Although TPI is a global organization maintaining a network being employed by roughly 3 million daily users[5], its annual budget is actually tiny. Between 2007 and 2015 the total revenues collected amount to a figure of $16.065.436 with an average of $1.785.000 per year. Year after year the economic resources available to the organization have grown constantly. In 2007 TPI's budget lined up at $452.725, in 2008 it was $531.105 and reached the figure of $1.041.633 in 2009, thus experiencing a spike of +96% in only one year. 2012 was a breakthrough year as well. In 2011 Tor Project collected $1.387.054 (more or less the same amount raised the previous twelve months, $1.336.308) but in the following fiscal year it almost doubled its economic resources, increasing its budget to $2.608.833 for a total increment of +88%. In 2015 the Tor Project's revenues were $3.278.452.

The vast majority of TPI's income is public money, mostly provided by US taxpayers. Indeed, between 2007 and 2015 83,86% of the organization's funds ($13.475.031) came from Washington: a small part of it – that is $2.164.008 or 16,05% – has been directly provided by the US government, while the remainder ($11.311.023, that is 83,94%) came from institutions and organizations tied to it. In this same period, the only non-US public institution that have funded Tor is the Swedish government which, via the

Swedish International Development Cooperation Agency (SIDA), provided an amount of $579.840 (3.60%). The rest of the budget have been provided either by US and European private foundations ($553.193 that is 3,44%) and other forms of contribution ($1.149.300, namely 7.15%). A small part of the money ($196.000 or 1,22%) has its origins in Tor Solutions Corporate, a consultancy company owned by TPI, founded in 2012 and dissolved in April 2016, after two years without revenues. Finally, a tiny fraction of the Tor Project's revenue came from other sources, named in the financial statements under the budget items "Investments" ($14.249, that is 0,08%) and "Miscellaneous" ($24.784 or 0.15%).

In the time span taken into account, Tor earned most of its income by applying for grants issued by US public institutions. As Tor people and members of the community have often claimed on the occasion of public events[6], the organization relies on three main different funding sources: the National Science Foundation (NSF), the US Department of Defense (DoD) and, particularly, the US State Department (DoS), along with a bunch of organizations linked to it. As it was explained in December 2017 by Roger Dingledine during a public talk he kept at the Chaos Communication Congress these funds are used to achieve different goals. NSF funding are employed for solving theoretical problems, such as those related to the infrastructure scalability and security. DoD money is used with the goal of helping users to be safe in situations of conflict while, talking about DoS funding, Dingledine made reference to this money as a resource being employed "to explain people how to be safe and what that means". As it will be properly detailed in chapter 5, NSF resources are free of bureaucratic constraints and, as such, they are largely preferred by the Tor Project's members. On the contrary, DoD and DoS adopt a milestone-based funding model which, as we will see, presents several shortcomings from an organizational perspective.

3.4. Universities, army, diplomats and activists

The first big funder of Tor is NSF. Between 2010 and 2015 the NSF has provided $736,573 to the Tor Project (4,58 % of its total revenues). More than half of this money (56,28% or $414.593) has been directly donated to the organization, while the remainder has been distributed through Drexel University and University of Minnesota. The NSF grant program that Tor benefited from is the "Computer and Information Science and Engineering award" (CISE), classified with the number 47.070 under the US Catalog of Federal Domestic Assistance (CFDA). According to the US General Service Administrator (GSA) website[7], CISE is aimed at reaching several goals, like: "to support investigator-initiated research and education in all areas of computer and information science and engineering; advance the development and use of cyberinfrastructure across the science and engineering enterprise; and contribute to the education and training of future generations of scientists and engineers who will dedicate their careers to advancing computing and information research and education as well as cyberinfrastructure". CISE's annual budget is close to 1 billion dollar: every year more than 8000 applications are brought to its attention, with about 1800 awards made in hundreds of different universities and colleges[8].

The second main source of funding for TPI is the DoD. After having funded the Tor protocol early development via NRL and DARPA, since 2011 the DoD have decided to contribute even more to the growth of the network by providing $3.726.090 to TPI (roughly 23,19% of the overall funding). According to the financial statements, the DoD has never directly donated money to Tor: on the contrary, it has always resorted to Stanford Research Institute International (SRI) as pass-through. SRI is a client-sponsored R&D and innovation center: according to a 2013 fact sheet, it is funded by the DoD for about 63% of its overall budget[9]. 76,43%[10] of the money provided by SRI to the Tor Project is classified under the CFDA 12.335. As stated on the GSA website[11], the name of the grant program falling under this code is "Navy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance" (also known as C4ISR). C4ISR is managed by the Department of Navy's Space and Naval Warfare Systems Center (SPAWAR), an organization with "more than 10.000 active duty military and civil service professionals [that] develops, delivers and sustains communications and information warfare capabilities for warfighters, keeping them securely connected anytime, anywhere" and "focuses on capable and secure communications and networks that span platforms and facilities[12]". Among C4ISR's objectives there are the following ones: "To support basic and applied research at educational, nonprofit, or commercial research institutions, which have potential for leading to the improvement of military operations or dual-use application, and to support training and stimulation of future researchers in science and engineering disciplines".

The DoS is the last and biggest funder of Tor. Between 2007 and 2015, it provided $9.012.458, corresponding to 56,09% of the overall Tor's budget. However, less than 20% of this sum has been directly transferred from the DoS to TPI: indeed, in 2013, 2014 and 2015 this money was provided by the "International Program to Support Democracy, Human Rights and Labor" (IPDRL), classified under the CFDA code 19.345. According to the GSA website[13] this money is managed by the Bureau of Democracy, Human Rights and Labor (DRL). In its own words, "the DRL leads the U.S. efforts to promote democracy, protect human rights and international religious freedom, and advance labor rights globally"[14]. This institution asserts to work in order to promote the advancement "of human rights and fundamental freedoms online through a diverse set of Internet freedom policy and programming activities". In order to do this, the DRL keeps "a 'venture capital approach' to its Internet freedom programming and invests in diverse responses to Internet repression". More specifically, its mission is "providing seed money for new ideas as well as supporting more-established programs that could scale rapidly and have high impact" and working "through bilateral and multilateral engagement, partnership with civil society and the private sector"[15]. The funds falling under the CFDA 19.345 is aimed at supporting "democracy and human rights programs to address human rights abuses globally, where fundamental rights are threatened; open political space in struggling or nascent democracies and countries ruled by authoritarian regimes; support civil society activists worldwide; and protect at-risk populations, including women, religious minorities, disabled, indigenous, and lesbian, gay, bisexual and transgendered (LGBT) people. In addition, DRL funds efforts across the globe to facilitate successful and sustained transitions to democracies, where civil and political rights are respected, and there is a process for transitional justice, accountability and reconciliation". IPDRL can rely on a huge amount of resources. According to the site usaspending.gov[16] which keeps track of the public money being spent by the government in federal programs, between 2010 and 2020 the DoS has invested only in this program just under 2 billion dollars[17].

The remainder of the funds that the DoS donated to Tor was provided via three non-profit organizations: Radio Free Asia (RFA), the International Broadcasting Bureau (IBB) and the Internews Network (IN). In 2012, 2014 and 2015 RFA donated the amount of $1,769.724 (20.5% of the money provided by the DoS to Tor). RFA is a US non-profit international corporation funded by the DoS: it was created in order to advance the U.S. foreign policy goals by broadcasting political contents, online news, music, commercial advertising and commentary to listeners in East Asia. The second one is the International Broadcasting Bureau (IBB), whose donations took place between 2007 and 2013, and they amounted to the figure of $2,351,400 (27%). IBB is a U.S. independent agency which acts as a technical support outlet within the Broadcasting Board of Governors (BBG). Finally, the biggest chunk of the DoS money provided to Tor (32%) comes from the Internews Network (IN): between 2009 and 2015, it helped the development of the network with $2,760,979. IN is an international non-profit organization incorporated in California that works "with citizens and local media in more than 100 countries. Together with local partners such as universities and other non-profit organizations, IN has supported the development of thousands of media outlets worldwide, including radio and television stations, newspapers, mobile news networks, and online news sites". Although formally independent, IN is completely funded by the DoS.

In the years going from 2007 and 2015, DoS, DoD and NSF grants roughly represented 84% of the total Tor budget. The remainder of the revenues came from the already mentioned SIDA, Google (from 2008 to 2010 the company donated $62.583), individuals and a plurality of private foundations. Among these latter, those explicitly mentioned in the financial statements – whose support to Tor can be quantified in $490.610 – are the following: the Electronic Frontier Foundation ($46.699 in 2007), AccessNow ($20.000 in 2012), the NLnet Foundation ($81.210 in 2008 and 2009), Human Rights Watch ($50.103 in 2007), the Knight Foundation ($252.181 in 2012), Stichting NiNet ($81.210 in 2008 and 2009), the Foundation for Christian Stewardship ($10.000 in 2012) and ITT ($93.000 in 2009 and 2010). The Tor's sponsors page[18] lists many more organizations among the funders of the network (like the Ford Foundation, the web companies Disconnect, Team Cymru, Shinjiru Technology, the National Christian Foundation and “an anonymous North American NGO”) even though their names are not explicitly mentioned in the financial reports that I took into account. Because of this reason, it is not possible to exactly quantify the dimension of each economical contribution to the project, nor the exact amount corresponding to the individual donations: however, according to what is reported on the documents, 7.15% of the overall funds (that is 1.149.300$) are listed under the voice ‘Other Contributions and grants’.

From this data some relevant points for the purposes of this research emerge.

a) As already mentioned in the opening of section 3.3, the budget available to Tor is tiny if we consider that the network was designed to escape the electronic surveillance of powerful opponents (such as ISPs, law enforcement agencies or nation states).

b) The money provided to Tor has been deferred in many small sums distributed over time. This rationale recalls that of the CHACS’s research agenda already discussed in the chapter 1, according to whom cyber-security problems must be addressed with a long-term perspective because, as its authors wrote, "dumping a large amount of money for a short period of time [will not] lead to a solution. System will continue to increase in complexity, and solutions developed today will not work for tomorrow's system [...] A modest investment over 20 years would be much more productive than a major investment over 5 years" (McLean and Heitmeyer 1995, 9).

c) Tor's funding system, its mode of operation and the limits it presents are consistent with the picture painted by Eghbal and the other authors previously mentioned in this chapter. In other words, Tor's situation is that typical of the FLOSS environment: a platform used by millions of people whose individual donations represent only a small fraction of the organization budget. Given the poor financial coverage that these ensure, the lacking of alternative revenues would necessarily result in the reduction of the Tor staff, with harmful consequences for the security and reliability of the infrastructure.

d) In the period taken into account the private sector showed a minor interest in supporting Tor development: the only company that provided some donations (and not even particularly relevant) was Google, while the overall contributions from charitable private foundations and individuals slightly exceed 10% of the total.

e) The creation of a consultancy company linked to Tor was a short-lived parenthesis that did not achieve noteworthy results in terms of project sustainability.

f) If Tor exists in its current shape, it is because over time several public institutions have decided to fund its development: the overall weight of US government public funds is absolutely preponderant in the organization budget. This applies to single fiscal years as well: for instance, in 2010 $1.241.321 out of $1.336.308 (92.89%) came from grants paid by organizations sponsored by the US government (IN, IBB and Drexel University). In any case, throughout the period taken into account, the yearly funds provided by the Washington political apparatus were never less than 68% of the total (as it happened in 2012, when the private charity Knight Foundation contributed to a significant portion of the budget with the sum of $252.181).

g) The Tor funding system is semi-centralized. Between 2007 and 2015, three big sponsors (SRI, IBB and IN) donated the sum of $9.114.409, corresponding to 56.91% of its budget[19]. In the same time span, the funds allocated by the DoD had a considerable weight in the Tor economy ($3.726.000, or 23.19% of the budget), even if they were not even half compared to those provided by the DoS ($9.012.458, or 56.09%, between 2007 and 2015).

h) The latter institution is a constant presence among TPI donors. It is worth noting that more than once its contributions allowed Tor to make a quantum leap. In 2012 TPI doubled its budget, thus covering a three years balance sheet liability which was starting to get heavy (–$214.170): by that year IBB's funds went from $150.000 to $387.800, while IN's support grew from $227.118 to $328.566. To these we have to add the money provided in the same period by New America Foundation ($25.000) and, particularly, by RFA through which OTF paid $150.000

> to Tor. In the following years, OTF became the Tor single largest donor, reaching the sum of $733.000 in 2014, $896.724 in 2015, $1.084.095 in 2016 and $798.029 in 2017. According to Tor's financial statements, between 2012 and 2017 the amount provided by RFA/OTF is $ 3,660,848[20].

Why have the DoD and the DoS funded the Tor network? The army's composite interests in building a T/A resistant network have already been articulated in chapter 1. For this reason, in the following pages I will focus on the DoS role: in order to explain the rationale behind the substantial economical contributions it provided for fueling the growth of the the Tor infrastructure, I will first analyze the OTF's annual reports published between 2012 (the year of its inception) and 2018[21]. Later in the chapter, I will interpret the data gathered in the light of the role played by media dissemination practices in US foreign policy since the 1960's.

3.5. OTF/1: connecting FLOSS with public funding

Established in 2012 and subsidized with the Internet Freedom funds being provided by the Congress, OTF is run by RFA and is overseen by the Broadcasting Board of Governors (BBG), a bi-partisan board ruled by the Secretary of State and responsible for the civilian media outlets sponsored by the US government (such as Voice of America, Radio Free Europe and the same RFA).

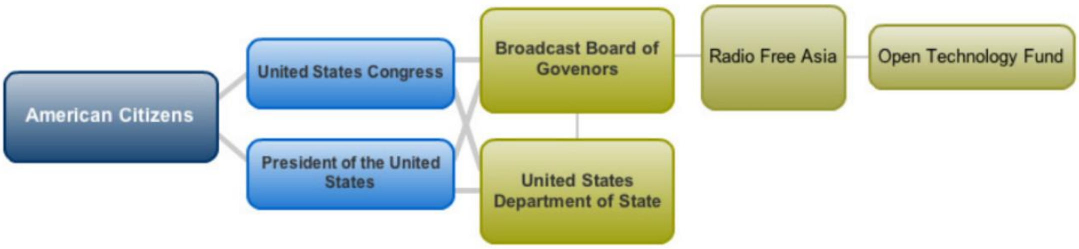
American Citizens
United States Congress
President of the United States
Broadcast Board of Govenors
United States Department of State
Radio Free Asia
Open Technology Fund

Fig. 12: OTF/RFA organizational hierarchy

With an annual budget ranging between 4 and 12 million dollars and a staff of 70 members, the organization operates in several countries like Burma, Ukraine, Iran, Afghanistan, South Sudan, Pakistan, Azerbaijan, Vietnam, Venezuela and China. According to the front page of its own official website "OTF supports projects and people that develop open and accessible technology promoting human rights and open societies, and help advance inclusive and safe access to global communication network"[22]. Among the values and principles driving its work, OTF's website mentions "a passionate support for the free and open Internet" and "the doctrine of open philanthropy and governance, to share openly with the public and other stakeholder in a non competitive fashion, all aspects of our work". Its mission is achieving a "long-standing positive change" by subsidizing "open technologies and communities that increase free expression, circumvent censorship, and obstruct repressive surveillance"[23]. In more prosaic terms, OTF can be defined as an incubator of digital security systems and protocols being funded with public money.

What makes OTF different from other public funders is the basic goal this organization was designed for, that is "increasing the accessibility of the US government Internet Freedom Funds to emerging talent by removing unnecessary barriers to entry, as well as growing capacity" and "attracting projects that do not meet the minimum levels necessary to receive support from others USG Internet Freedom Funders". Indeed, OTF is "open to individuals and entities based outside the US", as well as those "unable to incur the typical overhead accompanying a USG grant" or "lacking professional writing skills"[24]. It is worth mentioning what are the minimum criteria required in order to have access to OTF's funds[25]. Beyond directly supporting freedom of speech and expression, a project aspiring to be awarded with an OTF grant should be a software in beta stage without existent financial support. Also, it is crucial that it "integrates technologies that increase safety into commonly used software and platforms" and is not "limited to delivery of specific content". Its developers must be "interested in productive reviews and audits of their work" and "focused on a localized on-the-ground deployment". Moreover, as Fabio Pietrosanti and Giovanni Pellerano (founders of Globaleaks, one of the OTF's top projects) explained me, recently the organization has begun to ask candidates to define a long-term economic sustainability strategy, so that in the future they can further develop their software without applying anymore for public grants. Finally, it is worth emphasizing that the project owners can apply only for small amounts of money (usually ranging between $75.000 and $600.000).

OTF aims to support "low-cost yet high-return emerging technologies"[26]. According to 2013 annual report, 12 out of 20 projects were awarded with less than $150.000, while 2/3 of the candidates received less than $300.000. In the same fiscal year, 75% of the budget was spent in R&D while the remainder was used for implementing existing projects. Fiscal year 2016 roughly presents the same numbers, with the only difference that 7 out of 21 projects were awarded with less than 75.000$. These low spending thresholds along with a milestone-based funding model – devised so that the organization can keep track of the development process and disburse funds only upon the reaching of pre-established goals – allow OTF to minimize the possible risks resulting from its investments. Nonetheless, OTF executives deem as very valuable also an unsuccessful grant as it could represent the first step for a future success. Indeed, "by openly sharing its shortcomings, the project will reduce the likelihood that future developers repeat previous mistakes"[27].

Concept-notes that candidates submit to OTF are assessed by an advisory technical council in charge of reviewing them, as well as helping OTF to shape its annual program. In 2012 only 6 people were part of the council, while in 2016 they became 46. Year after year, the number of its members has grown along with the skills being made available to OTF, so much that today the advisory technical council almost looks like a think tank. Initially, this body saw the participation of a few ICT professional belonging to world-class companies with strong and long established ties with the FLOSS world (such as Twitter, Tumblr, Google and RedHat), as well as of a couple of US academics with computer science background. In 2016, the number of companies joining the advisory council has grown and their typology has become more diversified: indeed, along with the above mentioned companies, other important names joined it, such as Mozilla, Slack, Nielsen Norman (specialized in the analysis of the user experience and user interface) and the security firm Signal Sciences. Also, the number of academics who take part in it has increased along with their scholarly specialization: indeed, OTF's advisory council has started to host representatives from some of the most important US, Canadian and European universities, whose skills range from computer science to history, from political science to law, from cultural studies to journalism. Nowadays it is possible to find next to them several representatives of private foundations (such as Access, the EFF, the American Civil Liberties Union, the Wikimedia Foundation and the Linux Foundation) with a long-lasting expertise in the field of digital rights and open source. The advisory council also sees the participation of world-renowned intellectuals and authors (such as the cryptographer Bruce Schneier or the writer Cory Doctrow) and independent researchers, trained in social sciences, design or computer security. Moreover, several NGOs engaged in human rights protection and active in areas of the world characterized by the presence of authoritarian political regimes (like Middle East and North Africa) sit at the OTF's table: among them it is possible to mention Engine Room, Front Line Defenders, Amnesty International or Social Media Exchange. Furthermore, it is important to add that, not only OTF counts these important names in its advisory council but, in turn, the organization has its own representation in the "Linux Foundation's core initiative", which includes important names as well, such as Verizon, Samsung, Amazon, Google, IBM, Cisco, Intel and HP.

3.6. OTF/2: creating a global hacker community

It is unquestionable that OTF and Tor Project have a very special relationship. Indeed, if we exclude fiscal years 2012 and 2017, Tor has always been the project receiving the major amount of money from OTF, with figures varying from $500.000 to $900.000. More importantly, OTF's financial support to the project is both direct and indirect. Indeed, between 2012 and 2019, not only the fund has donated a substantial amount of money to TPI, but it has also funded other hacker communities, groups or individuals belonging to the Tor Community who have developed several security tools based on OR protocol, thus improving it or expanding its scope. So, along with the remarkable amount of $4.130.115 provided to Tor – money employed for improving the Tor protocol[28], the TBB[29], the Onion Services[30], the Tor Bridge distribution[31] and Tor Metrics[32] –, in the same period the RFA's incubator has invested $1.397.374 in OONI[33]. OONI's flagship software is OONI Probe, a cross-platform censorship measurement toolkit available for desktop and mobile (it runs on Android, iOS, Windows, Linux and Mac OSX). Initially released in 2011, OONI Probe is an application designed for detecting and identifying any technical measures being arbitrarily implemented by an ISP in order to filter or manipulate users' traffic. Run by thousands of people scattered all around the world, OONI "has collected millions of high quality measurements from nearly 200 countries using open methodologies, using FLOSS to share observations and data about the kind, methods and amount of surveillance and censorship in the world"[34]. These data are used as the raw base for periodic public reports about the state of online censorship in many areas of the world, with a particular focus on the Global South. Another Tor-related project funded by OTF ($208.000 in 2014) is Tails[35], a Linux-based live distribution, designed for individuals who need a high level of security and anonymity[36] (such as investigative journalist, activists or whistleblowers). Tails can be booted from a USB stick, it does not leave any traces on the computer on which it is run and the Internet traffic generated by a user is entirely routed through the Tor network. Globaleaks[37] is an open source whistle-blowing platform adopted by a growing number of NGOs, newspapers, public and private companies. Easier to set up than a Wordpress blog, Globaleaks can be made accessible through an onion service, thus providing whoever wants to submit a tips or a document without revealing her identity a high level of anonymity and security. In 2012, 2014 and 2017 OTF brought $452.840 to the hackers involved in the project[38].

However, these are just a few of the projects being tied to Tor and funded by the US taxpayers through OTF. Many other can be mentioned, such as NoScript[39] (an add-on for improving Firefox and TBB security, $350.000 between 2014 and 2017[40]); Briar[41] (a secure mobile instant messaging application relying on onion services to reduce the user-generated meta-data, $150.000 in 2017[42]); Cupcake Bridge[43] (a Chrome extension that "allows users to become new Tor bridges automatically, without having to install a full software suite or configure anything", $67.000 in 2013[44]), the Tor BSD diversity project[45] ("an initiative seeking to extend the use of the BSD Unix operating systems in the Tor public anonymity network", $40.000 in 2016[46]), The Tor Node Distribution Latam (a project seeking "to set up more network nodes in Latin American and grow the Tor user base", lately evolved in the NGO 'Derechos Digitales', $89.700 in 2017[47]) and Onions on Apple[48] (a grant provided for expanding the development of Onion Browser, "an open-source, privacy-enhancing web browser for iOS, utilizing the Tor anonymity network", $174.657 in 2019[49]). Moreover, in July 2017 OTF was the sponsor of the first

Tor bug bounty program[50] to encourage hackers and security researchers to find and privately report vulnerabilities that could compromise the anonymity of the network. The promised awards were up to 4000 dollars per bug, depending on its severity. Earlier the same year, OTF funded the collaboration of Tor with SimplySecure for the creation of a basic visual styleguide "to begin the work of creating a consistent visual look and feel across the entire project's ecosystem by standardizing fonts, colors, and logos"[51]. Also, OTF supported the creation of public events like the the OONIgathering[52] ($41.070 in 2017) and Internet Freedom Festival (IFF)[53] ($550.000 between 2017 and 2018). This latter is a meeting of hackers and activists who fight for freedom of expression. According to a public statement released by the Tor executive director, Isabela Bagueros, "so many projects from the Tor ecosystem benefited from that conference that is impossible to say it in just a few paragraphs"[54]. Last but not least, OTF helped with the growth of the network, setting up relays in areas of the world where Tor is traditionally not present. Indeed, as we can read in 2012 report, among the year key results the "deployment of the first high capacity Tor node in South East Asia" is mentioned.

Yet OTF funding activity goes far beyond TPI and the Tor ecosystem. Try to name any of the projects that emerged from the privacy activism scene in the last five years – or, at least, one among those that had a media resonance or a widespread diffusion – and you will find that it was funded by OTF. In 2014 and 2015, Qubes OS[55], a Xen operative system, based upon the innovative concept of security-by-compartmentalization, received a total amount of $570.000[56]. Between 2015 and 2016, Subgraph[57], a FLOSS security-oriented operative system aimed at defending non-technical users from high profile attackers (i.e. state sponsored actors), received $325.000[58]. In 2012, 2013 and 2015 Leap[59], a cross-platform and easy-to-use VPN and mail encryption client got $1.341.637 from OTF[60]. Wireguard[61], a new and secure VPN protocol recently implemented in the Linux kernel, was funded with $250.000[62]. The development process of Mailvelope[63] – a plugin for Firefox, Chrome and Edge that allows users to use the OpenPGP standard to encrypt their webmail when using providers such as Google, Outlook and Yahoo! – has been supported by multiple OTF's donations for a total figure of $261.000[64]. Lantern[65], defined in the 2014 report as a censorship-circumvention tool which relies on "peer connections as a source of Internet connectivity when servers are unavailable, and is particularly useful in repressive environments like Iran, China, and parts of Latin America", received support for $791.000[66]. In the two years period 2012-2013, Cryptocat, an end-to-end encrypted instant messaging client available for Windows, Linux and Mac got $184.000[67]. In 2017 and 2019, OTF funded the EFF's Certbot client[68] for Let's Encrypt ($236.400[69]), a project whose goal is making encrypted connections ubiquitous and available for each web server running on the Internet. More specifically, Let's Encrypt goal is to increase the Web overall security by making TLS certificates easily configurable and accessible: indeed, site owners do not need advanced technical skills to use Let's Encrypt nor they must pay an expensive fee anymore to a CA in order to implement their own encryption certificate. Finally, OTF has supported DNSPrivacy, a project seeking to further DNS encrypted services on the Internet that "provide data on the operational realities of DNS-over-TLS (DoT) and encourage mainstream DNS service providers to offer open, free DNS privacy services to the general public"[70]. Interestingly, since 2018 DoT has been implemented as default name resolution protocol in Android.

Nevertheless, the greatest OTF's success is by far the funding of Open Whisper Systems (OWS), the startup that created the secure messaging app Signal[71]. In 2012, when it got its first OTF contribution, this cross-platform application – currently considered as the end-to-end encryption golden standard in the instant messaging clients environment – was nearly dead. After four years of continuous development (and funding: OTF put $2.955.000 in the company run by the anarchist hacker Moxie Marlinspike[72]) the Signal encryption protocol has been reworked and re-implemented in the most important Silicon Valley instant-messaging platforms: Whatsapp[73], Facebook Messenger[74], Google Allo[75], and Skype[76] (along with Nextcloud[77], which is not a US product though). As proudly claimed in 2016 OTF report, the year "began with over a billion people already utilizing OTF-supported technologies, but ended with nearly two billion doing so". These results allowed Marlinspike's company to reach long-term sustainability, either because of the consultancy contracts he signed with the above mentioned companies and the creation of the Signal Foundation, financed with $50.000.000 by Brian Acton[78] (one of founders of Whatsapp, who made his fortune after Facebook bought his former company for 19 billion dollars[79]). It is no surprise that the economic sustainability achieved by OWS is a milestone being openly claimed by OTF in its 2017 annual report.

In the same document, OTF recalls that other platforms and "internet freedom tools [are] embedding Tor into their products". As a matter of fact, although not having achieved the popularity of Signal, Tor's protocol and software have been deployed in some of the major global communication networks as well. For instance, TBB is a version of Firefox that includes patches featuring anti-fingerprint and ant-tracking techniques being developed by Tor hackers. Once tested on TBB, such mods are mainlined into the Mozilla's web browser code and are used by dozens of millions of people, without them even knowing it[80]. Increasing Firefox privacy is one of the reasons because OTF funds Tor. As it is stated in 2013 annual report, the figure of $600.000 granted by the organization to Tor was aimed at identifying and fixing "current privacy and security issues in Firefox that impact TBB users", as well as improving "the usability and functionality of the Firefox extensions that are included with TBB". Similarly, OTF's support for preparing TBB for Android for mainstream adoption ($358.000 in 2019) is motivated by the will to preserve a strong bond between Mozilla and TPI, so that parts of the Tor code keep on being integrated into Firefox mobile[81]. Moreover, the attempt to implement in Firefox a "Private Browsing Mode" entirely based on Tor is underway[82], while Brave, a privacy-oriented browser based on Google Chrome, has already deployed such function[83].

With their advanced security and self-authentication properties, onion services are becoming pretty widespread among the major global ICT players and this is due to the OTF funding effort as well. For instance, in 2014 Facebook became accessible through onion[84] and, as stated in 2015 OTF annual report, it "extended its support for Tor users to Android through the OTF supported 'Orbot' app" (that is, a Tor client for Android developed by Guardian Project). With almost one million users per month, Facebook over onions "give people more confidence that they are connected securely" to the blue social network. In 2018 the Zuckerberg's company expanded its offer and increased the performance of its Tor infrastructure[85]. Cloudflare, one of the most important Content Delivery Network (CDN) and DNS on the market, recently deployed onion services into its own global infrastructure[86] and made it Tor-compliant[87]. Now, when a TBB user surfs a website delivered through the Cloudflare's CDN, its contents are always provided through an onion service. Microsoft is experimenting with onions and Internet of Things as well[88], while the Guardian Project used them for securing the domotic open source platform Home Assistant (this latter has been designed to work with systems like Amazon Alexa and OK Google)[89].

The data being available so far clearly reveal the purposes OTF has been conceived and designed for. *The first one has been that of filling a gap*. In fact, OTF is primarily a public technology incubator being specifically created to address the lack of an organizational structure within the US government which is able to intercept FLOSS hacker communities (particularly those ones being made up of people who produce encryption and censorship-circumvention software) and establish profitable relationships with them. OTF is a fluid, light and composite structure because these are the very characteristics of the environment with which the organization is called to get in touch. A world being made up of a dust of individuals and small affinity groups and being marked by dynamics of informality, decentralization, spatial dispersion, nomadism, where technical excellence, libertarian countercultures and unruliness coexist without ever contradicting each other. As we have seen previously, such world is dominated by a chronic lack of funds and suffers an objective difficulty in obtaining them, either because of its above mentioned structural features and the lack of an organizational interface that allows it to have access to public money provided by the State for fueling technological innovation. As a matter of fact, when in 2012 OTF was born, the DRL's Internet Freedom Funds could only be provided to US-based organizations, recognized by the law (like NGO, university or private companies) and never for an amount lower than $500.000[90]. These eligibility criteria are largely incompatible with the FLOSS ecosystem and in fact they represented a barrier that prevented certain sectors of the US government from getting in touch with it and exploiting its potential. OTF instead acts to create a bridge between Washington and the open source software developers, without asking them to lose their true nature, to give up their ethics of radical sharing, nor to spend time and energy in order to create a formal organization or to acquire grant writing skills just to send an application (without even having any guarantee of success).

With a simplified proposal submission process[91], OTF lowers entry costs to the market which, otherwise, would not be affordable for FLOSS developers. It does so by offering them a funding model being free from the set of problems typically affecting crowdfunding or individual donations system. The economic sustainability guaranteed by the RFA's subsidiary is not flawless (I will give an account of its operational problems in chapter 5) but at least it ensures coders an income that allows them to work within a less precarious time horizon, to develop their projects on a ongoing basis – not only the night or in spare time, as instead it usually occurs in all the New Economy sectors (Lovink 2008, 3-35) – and, perhaps, even to make them self-sustainable in the long term. In short, OTF is one of the possible answers to the question "who pays for open source?". Without the funds allocated by it, the wealth of projects like Tor, Signal, Globaleaks, Tails, OONI, Wireguard, Leap would have been lost – probably abandoned on some GitHub repository tagged as "Archived" – and their code would never have reached the maturity being required to go beyond a small circle of hackers, privacy activists and political militants.

But the role of OTF goes far beyond that of a simple funding agency. Its venture capital-style approach – out of one hundred small, low-risk investments, one is enough to pay for the costs incurred – and its successes have made it a catalyst for ideas and relationships. Despite of a rather small annual budget (the highest amount being available to OTF in its history was that of $12 million in 2014), the organization has seen a continuous growth in funding requests (at the end of 2018 they were more than 900). Events such as the IFF are moments during which communities and individuals scattered all over the planet have the opportunity to meet, to discuss and to exchange ideas. OTF's advisory technological council has become a place of contact and coordination between the DoS, international hacker communities, activists, NGOs, universities and important Silicon Valley companies. OTF is at the center of all this: with its work it weaves a lasting network of relationships between US politics, Californian businesses and intellectual elites coming from emerging economies or countries hostile to Washington's interests. Furthermore, it also acts as a 'revolving door' between these environments, putting them in communication with each other and creating a network of connections and informal relationships that can be easily spent in a professional context. Indeed, OTF's organization chart lists the names of many activists, hackers and IT professionals who, once being introduced into this multifaceted environment, have been hired in important technology companies, or have got job positions in academic research centers or have started working for human rights NGOs. Or even, in some cases, they have found themselves simultaneously playing all these roles, acting as a bridge between these diverse environments.

In addition, with the choice of supporting for a few thousand bucks the development of inter-operable high-quality FLOSS security protocols – all of them are content-neutral, not tied to a specific platform or operative system, and easily implementable in the most popular apps and software –, OTF has became an important source of technologies and ideas for several Silicon Valley companies (who, not by chance, have been involved since day one in the process of evaluation of funding applications). In this sense, OTF is like a large car manufacturer's Formula One workshop: its highly specialized employees create prototypes being designed to be used in extraordinary situations (such as competing in a grand prix or communicating in an area of the world characterized by high levels of censorship) but, at the same time, easily implementable on daily use technologies as well (such as a subcompact or a mobile instant messaging service). And even if, metaphorically speaking, OTF's cars should not win their race (that is, to become a mainstream project used by millions of users) or, still worse, not even get to the starting pits (namely, to be released as stable software), the experience drawn from yesterday's failures will serve to better build tomorrow's car.

However, it is important to emphasize that OTF's organizational and funding model does not emerge out of nowhere but, on the contrary, it is expression of a specific historical contingency typical of US industrial policy which, since the end of the WWII, has traditionally attributed to the State the role of technological innovation catalyst. As a matter of fact, the DoS funded organization seems to present a line of continuity with the experience of another major US federal research agency, namely the DARPA. The organizational practices of this latter (Mazzucato 2012, 103-13) are consistent with those being elaborated by OTF. Both are born precisely to act as a ring of retroaction between individuals and organizations, as a proxy that connects different worlds. Both enjoy operational autonomy and are based on a flexible and decentralized organization model. Both fund the development of ambitious technological prototypes – whose transformation into a finished product could take years before finding a placing on the market – and take care of organizing events to put engineers and researchers in communication, so that they can discuss each other's ideas. Both consider an unsuccessful project as an asset to take advantage from, namely a form of knowledge that emerges from the worldly experience and that can be used to positively address future research, without repeating the same mistakes that lead to failure in the past. In other words, both are an expression of a State which, while working closely with the private sector, has an active role in directing and fueling technological innovation. According to Block (2008), DARPA’s goal was essentially to attract the best minds within public institutions and create a scientific community with a widespread presence in universities, the public sector and big companies. OTF in turn pursues this same goal but with an important difference: the organization does not want to create a *sui generis* scientific community but *an actual hacker community*. OTF does not organize just seminars but conferences structured in all respects as genuine hacker meetings (such as, for example, the Internet Freedom Festival). Furthermore, it tries to be a point of reference and contact, not only between researchers, academia and business, but also between geeks, activists, journalists and NGO for human rights. Finally, its role is not *sic et simpliciter* to help a start-up to sell its product on the market, but, actually, to help small crews of nerds to reach an economic sustainability by creating a business model compliant with their values and their radical sharing ethic, as well as by getting them in touch with large global ICT firms with already established roots in the FLOSS world.

Although the reasons that prompted Tor (and dozens more open source organizations) to establish a close relationship with some specific sectors of the US state should now be clear, there are still some important questions previously introduced that need to be answered. Why did the DoS (and not another federal institution or agency) decide to set up an organization such as OTF to create this dense network of relationships with the FLOSS world? What are the advantages the Dos benefits from it? What is the political agenda it pursues?

3.7. Internet freedom: a bi-partisan agenda

The reasons that, over the years, have led the DoS to financially support the development of Tor (and, as we have seen, of many other encryption and filter circumvention technologies) are many and require a complex explanation. Indeed, the rationale behind this choice has a long-standing origin resulting from an approach to foreign policy developed by the US at the end of WWII, constantly pursued until the present day and adapted from time to time in front of the emergence of new socio-technical conditions. As explained by Powers and Jablonski (2015), the dissemination of media and communication technologies – a goal to achieve, possibly with the help of the private sector – is a strategy that the US have begun to implement during the cold war both for countering the Soviet expansion and for promoting the integration of the Global South into the western sphere of influence. According to the two scholars, this approach grew out of the modernization theory and it identified the diffusion of media contents and communication networks as fundamental premise for establishing free-market economies in so-called "underdeveloped countries". For his part, Nye (2005, 58-59) argued that the existence of radio stations such as Radio Free Europe or RFA – both created with the goal of broadcasting US propaganda and promoting American and European cultural product beyond the 'Iron Curtain' – has strongly contributed to spread western values and ideas in the former Soviet republics, so much as to be a crucial factor for triggering a democratization of the way of life in Eastern Europe, thus accelerating the end of the socialist regime. As explained by Morozov (2011), in the US diplomatic milieu this strategy is deemed so important that still today the fall of the Berlin Wall is not always interpreted as the result of the disastrous economic conditions which had affected the Soviet economy, but rather as an effect of the diffusion of samizdat, photocopiers, faxes, video recorders that had made the corrupt soul of the socialist apparatus transparent and visible, thus fueling a sense of dissatisfaction which soon turned into revolt.

This approach to foreign policy had an important evolution in the 1980s, when George Pratt Shultz, secretary of state during the Regan era, suggested an extension of it to the then nascent digital industry. In the essay "New Realities and New Ways of Thinking", published on 'Foreign Affairs' at the dawn of the second presidential term, Shultz went so far as to argue that the affirmation of the ICT market was "challenging the very concept of national sovereignty and the role of the government in society" (1985, 715). In his view, the very existence of such market sector was due to the implementation of specific neo-liberal government policies – such as decentralization, deregulation, tax exemption and denationalization –, whose result had been "to reduce rigidity […], enlarge the scope for individual producers and consumers to cooperate freely through market" and "give free rein to entrepreneurship, as the wellspring of technological creativity and economic growth" (ibidem, 715). In light of the ICT success – and in order that the expansion of this market sector could continue over time – public institutions were called to rethink their role. No taxes, no controls, no regulations had to hinder the flow of electronic information. On the contrary, according to Shultz the only purpose of the State should have been to encourage the creation of an international "open system", designed to protect the individual initiative from any form of interference, including that deriving from the exercise of national sovereignty – from which the same government should had to withdraw in order to make room for individual entrepreneurship. In the long run, Shultz wrote, the effects of this "open system" would have been disruptive on the international scenario as well. The non-democratic states that would have opposed it were destined to the economic disaster, while those ones that would have opened their borders to it would have been forced to implement a process of liberalization that would have undermined any hypothesis of authoritarian control over society. Therefore, the international system conceived by Shultz was not only an open system, but an opening system well: his project was to induce a reconfiguration of the international political order with the aim of deleting any political regime whose authoritarian characteristics would have made it incompatible with the very high technological concentration of the new ICT market, as well as with the process of democratization of society that this new economic sector would have necessarily required in order to thrive.

Also known as "the dictator's dilemma", since early '90s Shultz's vision became a political agenda whose main points have been reworked, refined, codified and eventually put into practice at the highest levels of the US government. As a matter of fact, from 1994 to 2017 every single Secretary of State, democratic or republican, has assumed the above mentioned strategic approach as one of the programmatic axes upon which the US foreign policy was based. On March 1994, during International Telecommunication Union's (ITU) World Telecommunication Development conference, vice-president Al Gore announced the Global Information Infrastructure (GII), that is a political initiative aimed at promoting the deregulation of the communication sector, the removal of trade protections and a surge of investments by US and European corporations and institutions in order to advance the growth of a global communication infrastructure[92]. In 1997, under the rule of Bill Clinton, the White House issued the Framework for Global Electronic Commerce, calling against government taxes, trade barriers, telecommunication constraints and other forms of regulation for Internet corporations[93]. In 2006 the Bush administration's Secretary of State, Condoleeza Rice, established the Global Internet Freedom Task Force (or GIFT) in order to increase "freedom of expression and the free flow of information and ideas", reduce "the success of repressive regimes in censoring and silencing legitimate debate" and promote "the access to information and ideas over the Internet"[94]. Interestingly, in doing so, she also established a "$500.000 grant program" supported by the DRL "for innovative proposal and cutting-edge approaches to combat Internet censorship in countries seeking to restrict basic human rights, including freedom of expression"[95]. During the Obama's administration, Hillary Clinton went even further: during two notorious speeches given in January 2010[96] and February 2011[97], the Secretary of State equalized the access to Internet connectivity to a fundamental human right (as much as freedom of speech, freedom of worship, freedom from want and freedom from fear). Also, she renamed the GIFT in 'Net Freedom Task Force' and provided it with a budget of $145 millions in order to fund the development of encryption and filtering circumvention technologies[98]. As clearly indicated on the DoS website, this huge financing effort was inspired by the White House's International Strategy for the Cyberspace[99]. This programmatic document call the Internet's "self-organized community" for building an open, inter-operable, secure and reliable infrastructure based on standards determined by expert groups and aimed at supporting free trade, intellectual property protection and freedom of expression and association.

Called in many ways – Information Highways, Internet Freedom Agenda, Open Internet Agenda, Google Doctrine, Freedom-to-connect theory –, the one discussed above, is a foreign policy approach that resorts to a cyber-utopian rhetoric in order to promote a Neo-liberal political and economic agenda. Individual empowerment, strengthening of an imaginary global human community, equal opportunities, eradication of injustice, increase of the general level of well-being: in the words of the politicians that, one after the other, took office as head of the State Department, the Internet has always been represented as a driving force for economic growth and innovation because of its supposed universal ability to equalize access to information, knowledge and markets. For this reason, Evgeny Morozov (2011) argues, technological commodities have often been depicted as tools for fighting oppression and the companies providing them to the masses portrayed as paramount actors for making contemporary dictatorships more open, decentralized and participated. In parallel, the rhetoric of freedom of expression "has been the preferred usage of American corporate and monopolies, press and other, to describe the mechanisms of the system that favors their operation" (Nordenstreng and Schiller 1979, xiii).

Yet, as explained by Goldsmith (2018, 4), the concept of Internet Freedom has actually always been weaponized to "enhance the wealth of the US global firms", "export to other countries notions like free trade and free expression" and "impact policy abroad": if the Internet design is modeled on US values, says the scholar, it is because they could spread along with the implementation of the network, thus facilitating regime openness and regime change. Power and Jablonsky (2015, 24) express a similar opinion by saying that the Open Internet is essentially a particular conception of networking – depending on US companies, supporting Western norms and promoting Western products – elaborated for "legitimizing the existing institutions and norms governing the Internet industries in order to assure their continued market dominance and profitability". This dynamic is not new, as Bowker and Star (2012, 240) brilliantly summarized by recalling that "just as in the nineteenth century the laissez-faire economics of free trade was advocated by the developed countries with most gain (because they had organization in place ready to take advantage of emerging possibilities), so in our age the greatest advocates of the free and open exchange of information are developed countries with robust computing infrastructures. Some in developing countries see as a second wave of colonialism: the first pillaged material resources and the second will pillage information".

3.8. Undermining sovereignty, strengthening national interest

Within the strategic framework previously described, the State plays a fundamental role that is connecting non-western countries to western companies and markets (Assange 2014). How? Essentially by building new forms of legality, be them juridical or technical, being designed to facilitate the operations of US corporations, encourage their penetration into global markets and guarantee their ownership rights (Sassen 2008, 51). In turn, this objective can be pursued by following two different paths. First, as we have seen, by signing international commercial treaties aimed at increasing the liberalization of communication on the territory. Second, by fueling the development of technologies enabling Silicon Valley companies to have a secure access to global electronic markets, where necessary also bypassing the central authorities of individual national governments and reducing their ability to regulate their own digital networks by the rule of law. In both cases, the State has a fundamental role: drawing upon a strategic vision (the open system envisaged by Shultz and pursued by his successors), it implements industrial, fiscal, commercial and foreign policies to support the growth of national private companies and their expansion abroad. Moreover, by taking an entrepreneurial risk on its own (namely by providing non-refundable public money to emerging players on the market), it encourages the development of innovation hubs (such as OTF) where new technologies that make national companies more competitive are built (Mazzucato 2012, 103-4). This occurs because, as claimed by Sassen (2008b), in a context where power (be it political and economic) takes the shape of deterritorialized flows of money, information and knowledge, the role of the state is to encourage the deployment of globalization processes, either by deliberately withdrawing from the regulation of the economy and by loosening the 'national slots' that would prevent its full development.

The use of the onion routing protocol has been experimented in order to reach this latter purpose as well. When I asked to a few Tor people why they thought Facebook had chosen to make their portal accessible through an onion service, I received two kind of answers. The first one emphasized the fact that, despite Facebook is counter-intuitive from a privacy perspective, there are actually a lot of different threat models: in this perspective, giving away one's identity while concealing one's location fits a particular niche, as does evading censorship by accessing an onion service. However, a part this, another person stressed the potential benefits of Zuckerberg's company resulting from its choice to test Facebook over onions.

> "I guess that Facebook engineers have decided to experiment with a new authentication protocol capable of resisting traffic hijacking attempts which Beijing puts into practice on a daily basis against millions of users"

Let us be careful though. The relationship between the state and Tor (but the reasoning also applies to Signal and the other hacker communities fostered by OTF) requires a complex interpretation because it does not involve the US government *tout court* but only some of its specific sectors that benefit from this relationship. Other ones are excluded from it and are actually damaged by the fact that OTF, NSF or DoD have fostered the growth of the FLOSS ecosystem being described in the previous pages. As often many Tor people have told me, "the US federal state is not a monolith: some of its agencies have every interest in collaborating with us, while others are willing to destroy us".

The truthfulness of this claim clearly emerged in 2016, when one of the OTF sponsored technologies, namely the Signal protocol, became subject of public debate in the US. After the S. Bernardino attack – and the strong demands made by the FBI because Apple decipher the iPhone belonging to the terrorist who had conducted it – Facebook chose to take a public stance against the pressures exerted by the Bureau. It did so by implementing the Signal protocol into the Whatsapp infrastructure. Over night billions of users began to exchange messages that could not be deciphered by Whatsapp, nor the FBI or any other government agency, but only by the legitimate phones owners. This choice involved considerable advantages for the Zuckerberg’s company. Since the Signal protocol makes it impossible for anyone to read the messages being exchanged – encryption keys are exclusively stored on users' phones – it would no longer have made sense for hackers, criminals or state-sponsored actors to attack the Whatsapp infrastructure in order to get hold of such messages. Furthermore, since Whatsapp cannot provide information that it does not have, the implementation of the Signal protocol has to be deemed as a form of protection of the Whatsapp infrastructure also from another perspective. Indeed, it makes it impossible to answer court orders that require access to users data for ongoing investigations. If we consider that Whatsapp operates under hundreds of jurisdictions, it is clear that the choice of deploying this end-to-end protocol on a global scale not only represents a form of shielding against undue political pressures, but also a significant saving in terms of legal expenses.

This move unleashed a fierce confrontation. Although the story was represented in the press as a clash between the Silicon Valley and the State, a more careful reading of the statements being made in those days by Washington's officials shows that the ongoing conflict was mainly between the same members of the government. As argued by a senior administrative, who spoke to ‘The Christian Science Monitor’ under the condition of anonymity, the issue “engendered a robust debate” in the corridors of power and the “government versus tech narrative” had to be considered as a “mischaracterization”[100]. The Federal Bureau of Investigation (FBI) and the Department of Justice (DoJ) took a very tough stand against Californian Internet Companies and called for their regulation by adding backdoors to cipher algorithms, so that they could have access to encrypted media whenever it was required for investigative purposes. Interestingly, many other governmental agencies openly opposed and turned down this option. In an interview released in March 2016, the Defense Secretary Ash Carter described encryption as a matter of national data security: “that’s how we make ships, planes, tanks, soldiers all talk one another. And so we need good data security. Therefore, we are on the side, absolutely, as the whole government is, for strong encryption”. Moreover, he also depicted encryption as a mean to keep the Internet compliant with US interests: “Russia and China openly defy all the values of freedom of speech, of free and open Internet. If they write the rules, they won’t be consistent with the values of the United States”[101]. “Why would you weaken a powerful cyber tool… even for a legitimate law enforcement?” claimed the former NSA director Micheal Hayden. Similarly, James Clapper, director of the National Intelligence, defined digital attacks against business and critical infrastructure as the most dangerous threat for the US[102]. Julie Brill – former director of the Federal Trade Commission (FTC), the law enforcement agency responsible for protecting consumers – framed the problem as a matter of business security. Strong encryption, she stated during an event organized by PassCode, "it's to protect critical infrastructure, or enterprise data or consumers data". Another commissioner of the agency, Terrel Mc Sweeney, claimed encryption is crucial for favoring the next wave of the ICT industry, that is the Internet of Things (IoT): without the consumers' trust in such technology it is unlikely they are going to connect their houses, their cars and even their bodies to the Internet[103]. Also the White House repeatedly expressed its concerns about encryption weakening or regulation. In 2013 an official report asserted that the government should not "in any way subvert, undermine, weaken or make vulnerable encryption"[104]. In 2016, it declined to push for a legislation update about wiretap laws: "I am skeptical of Congress ability" said Josh Earnest, the White House Press Secretary "to handle such a complicated policy area given Congress's recent inabilities to handle simple things"[105]. A problem being made even more complex by the fact that, as claimed by Ed Felten, deputy Chief for the White House Office of Science and Technology Policy, US economic competitiveness, privacy and human rights "are all big deals and they don't all point to the same direction from a policy perspective"[106]. The fragmented configuration of interests and powers described by Felten is typical of a de-nationalized state (Sassen 2008, 48-9). Its structure is characterized by a provisional cohesion due to the fact that some groups belonging to it (like DoS or DoD) achieve hegemonic control over others (like DoJ or FBI) because of their direct participation to the development processes of the global economy (for instance, by helping to build its technical and juridical infrastructure).

3.9. Conclusions

As we have seen, the relationship between the US State, OTF, Tor and other hacker communities being committed in the creation of encryption and censorship-circumvention tools is so complex that it requires several reading keys in order to be fully understood. Let us try to summarize them.

a) The breeding ground for the financial support of projects, such as Tor, Tails, OONI, Signal and many more, has been made possible by the coexistence of numerous historical contingencies, policies, political economies and geo-political scenarios that affect a 75-years time span. In this perspective, the most notable elements mentioned in the chapter are undoubtedly the FLOSS poor economy, the entrepreneurial role traditionally played by the US State, its political efforts being pursued to configure an Internet governance model favorable to the Silicon Valley and the Open Internet Agenda. Tor's funding system and its rationale are therefore part of a complex system of events that cannot be simply attributed to a single political actor or univocal will (as instead claimed by Levine, 2017).

b) The money provided by OTF has several functions. The first one is to create a hacker community scattered on a global scale and made up of talented individuals, groups and organizations. This community is at the core of a system of communicating vessels that connects different areas: the Silicon Valley, the academy, big public research centers, the DoS and NGOs for human rights. With its scouting and community-building work, OTF creates a network of informal relationships within which a virtuous process of training, circulation and osmotic exchange of ideas takes place.

c) The existence of this network also translates into the creation of professional opportunities for those who belong to it. Once joined it, a coder or activist coming from the hacker underground scene finds herself included in an environment populated by high-ranking ICT professionals, internationally renowned intellectuals, academics from prestigious universities, members of important NGOs and public sector officials: these are all contacts that can easily turn into profitable working opportunities. For sure, the opposite reasoning also applies: Californian firms have every interest in being present in this milieu of geeks so that they can directly get in touch with some of the best minds in the field of digital security and, possibly, to recruit them within their staff.

d) OTF network also represents a channel of communication between the DoS and the dissidents of countries traditionally hostile to the US (or in which economy liberalization is hampered by local authorities). These are cultured, tech-savvy, lay and westernized youths, in all respects resembling the ones who in 2011 leaded the so-called "Arab spring" in several Middle East countries. According to Formenti (2012, 134), in the eyes of the US administration and corporations, they are the most suitable candidates to replace the old authoritarian regimes with new elites who can ensure "at the local level, the interests of the global capital that today has more complex needs than those of the old oil companies".

e) OTF public grants fuel the research and development of innovative open source encryption, authentication and security protocols which, as we have seen, can be implemented for free by Big Tech firms in order to secure their infrastructures, both from a technical and legal perspective. Furthermore, the fact that Silicon Valley companies adopt in their platforms protocols widely considered as privacy and security golden standards, increases users' confidence in their work. For these companies, the projection of a positive image, and the trust that derives from it, are assets to preserve. They make profits on data that users upload to their servers: if they stop doing it because Silicon Valley’s reputation falls down, in the long run also their revenues could do the same. On the contrary, a cheerful and confident user produces more data.

f) Strong encryption protocols do not have a unique value in the eyes of the various institutions and agencies that belong to the US government. Some of them (such as the FBI or the DoJ) are penalized by their development and mass diffusion, because these make some traditional investigative techniques ineffective. Instead, other state sectors (such as the army, intelligence agencies, the FTC or the White House) actively support research in this field because they identify encryption as a suitable tool for protecting the national security and strengthening the country's military and commercial infrastructure.

g) For the DoS, encryption and onion routing are tools that contribute to keep the Internet open (that is to say free from state interference) and, as such, compatible with a governance model that favors the operations of large US corporations on a global scale. By opening firewalls and making harder for national governments to watch their own citizen’s data, these technologies become tools for pursuing disruptive politics towards countries hostile to the US

> (like China, Russia or Iran to name a few). Networks such as Tor, Leap or Lantern allow activists and dissidents to be able to use communication and organization infrastructures that are not controlled by local governments and companies. Also, they provide access to media outlets, websites and western social media that are usually off-line because of the restrictions imposed by national authorities. In this perspective, these networks represent a field of experimentation for US Internet companies in order to gain access over foreign markets that would otherwise be foreclosed.

However, in order to close this chapter and to introduce the next one, I would like to spend an important word of caution and to make some considerations explicit in regards of what has been written so far. As stated in chapter 2, at the heart of the methodological approach that I have used in order to conduct this research there is the idea of infrastructure as relational concept. Just as a plumber gives a tap a different value than a cook does, a DoJ official attributes to Tor a different meaning than that being given by a DoS official. However, these different ways of seeing the network, this interchangeability of meanings that Tor has in relation to organized practices does not interest only the different souls of the US government, but it is a phenomenon that involves also the same people who have built the infrastructure over the years. For instance, the fact that the DoS sees Tor (and more generally encryption and security technologies) as a tool to facilitate the US penetration in hostile countries, does not mean at all that the hackers who have materially written the code of the infrastructure fully embrace this vision. Some of them (actually very few) ignore it, some others share it, while some others else (in my experience the vast majority) believe that the effectiveness of this strategy is somewhat limited (not to say null). Yet, they think that a collaboration, especially if indirect, with Washington and some US companies, provides more advantages than disadvantages, allowing them to carry out the development of class A software projects, often widely employed by radical political communities. As a matter of fact, although it is true that onion services are seen by Silicon Valley actors as technologies aimed at increasing the security of their platforms or as tools for getting an unregulated access to electronic markets, it is nonetheless true that for years their capability to undermine the traditional state authority has been put at the service of global communication infrastructures being linked to the world of social antagonism (such as Riseup[107], Autistici/Inventati[108] and Systemli[109]). Similarly, although it is indisputable that Signal has become a security golden standard for diplomats all over the world, it is also true that this same app experienced a surge of downloads in the US during the street demonstrations which took place after the murder of George Floyd[110]. Just to make another example, during the invasion of Rojava (Northern Syria) occurred in the first months of 2018 by the hand of the Turkish army, I found myself configuring a few private bridges, PTs and onions in order to safeguard the connectivity of some journalists who were using Tails and Signal in order to report what was happening on the ground. In short, in the context of that terrific power imbalance afflicting the Internet, these technologies – although partly compliant with the US neo-liberal hegemony project – act as a power equalizer. In short, in the context of that terrible imbalance of power characterizing the Internet, these technologies – although partly compliant with the US neo-liberal hegemony project – act as a power equalizer. Indeed, they give back to individuals and groups with limited resources the possibility to enojoy a condition of anonymity and security which otherwise they would not be able to benefit from in normal conditions (and even less in exceptional ones).

Denationalized state, entrepreneurial state and Open Internet Agenda are just some of the pieces of this complicated puzzle called Tor. With Edwards' words, we could say that they are elements of macro scale that define the historical context within which the infrastructure is situated and which, in turn, is shaped by the infrastructure itself. Their analysis is certainly pivotal but far from being enough to paint the whole big picture of Tor. Now I want to broaden the range of analysis and move to the micro level by bringing to the foreground the many concepts of privacy, often very different to one another, which the Tor developers have tried to embody into the network. The next chapter is about this topic.

4. Privacies

4.1. Introduction

During my research, I interviewed twenty people who play (or have played) an active role in the Tor Project or in the management of its infrastructure. The discussions I had with them usually ended up on a specific point – that is to say, the meaning they attributed to the word “privacy". Confronted by this question, my interviewees have always reacted showing a certain discomfort, which was ranging from embarrassment to skepticism, from coldness to open irony. Specifically, one of the Tails developers welcomed the question with barely concealed giggles, that inevitably ended up affecting me too. His answer, similar to others that I had previously received, sounded more or less like this: "As for me, and for what my background is, it is far easier to point the finger at surveillance, rather than talking about privacy". This unease in dealing with the topic was also mirrored by the fact that, when faced with this problem, the interviewees – until that moment very talkative and open to discussion – suddenly became of few words, as if they were trying to avoid the point and to skip to the next question as soon as possible. Why? Why did hackers, engineers and activists engaged (in some cases for more than 10 years) in the development of a privacy-oriented infrastructure seem not to be eager to talk about privacy?

The answer is that discussing privacy in abstract terms, as if it was an absolute and uniform value, independent of the reality in which it is located, is simply impossible. As a matter of fact, the meaning of this concept is not fixed, but it changes according to the cultural trends of a given historical period and differs from one society to another: acknowledging such variation is the first required step in order to deal with the problem of privacy and understand it (Lyon 1997). Furthermore, this uneven interpretation does not only pertain to the cultural dimension of privacy, but it extends to the legal one as well. Indeed, although in many jurisdictions it is a widely recognized right (in some cases privacy has the value of a fundamental right, in others it is acknowledged as right of constitutional relevance, in others as human right) its legal framework suffers a substantial weakness due to two fundamental problems: the inadequacy of national rules in a global context and, particularly, the stasis of the law in front of the dynamism of technology, which makes it difficult to establish even minimal jurisprudential concepts (such as that of data ownership) (Weber 2012). In fact, the new forms of digital surveillance have gradually challenged the concept of privacy, the balances upon which it has been built, its meaning and also the usefulness of its traditional formulation in the current historical context (Rodotà 2004; Bennett and Parsons 2013). For instance, Ippolita (2017) argued that the current Internet configuration denies by default "the right to be left alone" (meaning originally attributed to the word "privacy" by the jurists Warren and Brandeis in 1890). Instead, according to Stalder (2010) since the new forms of sociability are intermediated by digital networks, the need to create a separation barrier to protect the individual's inner sphere has faltered. This is because it is precisely her ability to progressively disclose her personal information that allows her to be part of a network of peers characterized by mutual trust. In other words, privacy has become a factor of exclusion from the network and, for this reason, the role that it had historically played (namely safeguarding personal autonomy in front of the intrusions of power) disappears. At the same time, surveillance practices being undertaken by Internet companies are not perceived as a form of domination but rather as a service being aimed at providing visibility to individuals and, thus, guaranteeing their mutual interaction. Whatever way it was conceived in the past, nowadays privacy is closely linked to the concept of digital surveillance (Lyon 2002), so much as to be considered as a by-product of it: indeed, it is almost exclusively defined in relation with state practices being employed to violate it. As such, it has taken on the characteristics of a responsive and non-progressive concept which is impossible to theorize in a creative way (Cooke 2015; Lewis 2017). Moreover, it is worth noting that the traditional conceptualizations of privacy arise from an effort primarily being aimed at defining its essence and foundational features: unfortunately, the results of this approach have been disheartening and they have produced a plurality of inadequate definitions that fail to include (or exclude) from their boundaries aspects of life that usually are being considered as private (Solove 2008). Finally, this quagmire of conceptualizations not only has shown to be useless for prescribing solutions and for addressing privacy-related problem but, on the contrary, it has created new issues: in fact, the attempt to link privacy with high-order values has introduced conflicts with other high-order values (for instance, freedom vs national security) (Nissenbaum 2009). In summary, I believe that the awkwardness experienced by my interviewees in dealing with the problem of privacy, is explained by the fact that this notion has now become a conceptual shorthand to describe a cluster of problems that do not have a common denominator or a core element (Bennett 2011).

For this reason during the interviews I chose to adopt a different approach and, by receiving Nissenbaum's suggestion, I dealt with the problem of privacy in a more 'close' way. Since, nowadays this concept is increasingly subject to variations and unevenness that do not allow its univocal reading, the scholar claims that its value can emerge only through the observation of the practices associated with it, from a description of the activities that they make possible, as well as from the interpretation of their meaning in light of the context within which they are situated. Hence I stopped asking Tor developers 'what' was privacy, but rather I tried to bring out from their words the subjective meaning that they attributed to it, how this had emerged from their personal experience and how such meaning had been translated and embodied into the infrastructure that they had contributed to build. In other words, as I have detailed in the methodological chapter, I choose to adopt a biographical narrative approach, focused on the interviewees relation to hacking and, specifically, to the problem of privacy.

4.2. Making mistakes and exploring social boundaries

"... and my first PGP key dates back to 1995". With these words Moritz Bartl concludes the long story in which he recalls the key moments of his life which have led him to care about privacy, anonymity and online security. Moritz is a sort of institution in the Tor community. Being involved since the early '90s in the hacker counter-culture and free software movement, when he enrolled to university he chose to study Computer Science at the Technical University of Dresden, the only department he had found with a specific focus on Internet anonymity and privacy. Pupil of Andreas Pfitzmann[1], Moritz majored in software engineering and he soon became a teaching assistant. Yet, despite this enviable CV, he defines himself “not very good at coding” and, because of this reason, for many years he has focused on the organizational dimension of Tor (and more in general of online anonymity). Since 2010 he runs Torservers with his friends Jens Qubitzel and Juris Vetra. As stated on the homepage of the project, Torservers – backed by the German non-profit organization Zwiebelfreunde, which in German means ‘Friends of the onion’ – is a registered non-profit association and an independent global network of organizations[2], that helps the Tor network by running high-bandwidth relays. Beyond this, he is a Tor Project core contributor, director of the Renewable Freedom Foundation[3], fellow of the Hermes Center[4] and member of the Berlin-based Center for the Cultivation of Technology[5].

Moritz was born in 1982. He came into existence in a house (not in a hospital) and grew in an environment that led him to develop a consistent questioning of power, as well as a strong criticism towards the traditional German society and its educational system. At the time his mother was working in a bookstore in Munich and was very active in radical left movements, even though a few years later she will decide to quit them, being persuaded that they were no longer able to produce significant political and social changes.

> “She was part of a group made of people who started their own kindergarten, because the only kindergarten available had a kind of church background, very kind of traditional oppressive educational system, strong hierarchies. She was more in that wave of anti-authoritarian ‘Let the children do whatever they want to do’. They have no choice but to start their own kindergarten”.

Moritz grew up and, when he became a teen, he was forced to attend German public schools. The transition to the public educational system was traumatic. Unwilling to comply with the lifestyle that children around him seemed instead to follow to the letter, he kept clashing with teachers and peers, and he lived his adolescence as a "weirdo in a circle of weirdos". A situation made even more complex by the continuous re-locations of his mother who was used to choose temporary accommodations in buildings approaching demolition in order to save the money of the rent. This nomadic life forced Moritz to cut ties with friends and acquaintances every two or three years.

In this context he began to develop interest and curiosity towards the use of computers that, little by little, became central in his youth educational process. When he puts his hands on a Commodore for the first time he is 9 years old. In the first half of the '90s he started to use the Fidonet Bulletin Board System (BBS) and took part in the local scene of disk swapping, being made by thousands of people who shared software through a pretty traditional communication infrastructure such as the mail system. In this context he started to develop a flair for safety. It all began when an early crackdown on the German hacker scene lead to the arrest of a few "serial sharers":

> “At the time in Germany there was this lawyer who was used to honeypot people who share their software through a magazine (which was the ‘central node’ of this file sharing analog network). He created fake ads by saying: ‘Hello, my name is Tania and I do not know absolutely nothing about computer. Can you send me your list of pirated software so that I can buy it?’. The kids who fell into this trap and sent their list of software (usually attaching their name and address to it) were hunted down and sued. After these episodes I learned the first basic security measures, like not necessarily revealing your true name”.

In 1996 he bought his first modem and in 1997 he registered his first mail box. During high school, for a long time he was the only student who owned a CD burner, and because of this he enjoyed a certain popularity. He wrote his graduation thesis on the history of the Internet. He surfed the web in search of strange – and sometimes illegal – material to collect. Listening to Mo’s history means taking a dip in another era, when the Internet was not yet a mass medium, but a niche environment, reserved for a few insiders. In Moritz's eyes the fact that cyberspace was a hidden and little understood world was an element of fascination, which was in turn reinforced by another factor:

> “Since my mother removed herself more and more from the political scene… well, you know, this also had a bit of effect on me. Looking to society and

> how things work – and coming from this shielded environment and looking stuff from a distance, where you can a bit detach you emotionally but more look kind of the system – my motivation was not exactly political in that sense. It was more like already giving up on any change, and kind of more egoistical. Something like: 'This is all bullshit and I understand it is not going to produce change, I will not be able to change anything, but I can basically do whatever I want if I open this box'".

A concept he summarizes with the following anecdote:

> "When I was a kid, in Germany there was a magazine called 'The Data Pirate' a classical example of the zine scene: home printed and distributed via mail; I wrote a couple of articles for that magazine, I think they were about reverse engineer stuff. I got a bit into reverse engineering, remove copy protection, removing limitation of software… that's like you explore, right? It started like this. Instead the name of the program you put your name, because you edit the binary and you replace the string, without understanding anymore, you discovered hex editor, and you can edit the strings, and you start the program and your stuff appears".

At that time, digital technologies were seen by Moritz as esoteric and mysterious objects that provided those who handled them a certain power: they allowed to break pre-established rules – whether they be imposed through cultural conditioning, legal apparatuses or technological devices – and to explore unknown territories where it was possible to experiment new practices, to test one's skills and learn new knowledge, even those being normally considered not licit. In Mo's opinion, this kind of power is inherent in privacy-oriented technologies as well, since they enable people to create a space

> "where one can explore and do stuff. In the beginning it was just the kind of fascination of… I mean I started when I was 10 or something and then across, when you are 14 or 15, everyone has this kind of violation of certain rules, and for me it became an aspect for healthy society that people have to test its boundaries. […] If we have a society that is like in the US where kind of any violation becomes known and it is immediately seen a kind of criminal

> activity … well, this kind of society is a very oppressive society where you do not have this freedom. And you have to be very selective about what you share with other people. There is a difference between privacy and anonymity. Privacy is free space where you can decide who can to know, spaces where you can selectively reveal stuff".

In Moritz's view, Tor, like other privacy-oriented technologies, can provide its users a very specific power, that is to say that of 'making mistakes'. In Italian, this verb is synonymous of the term 'errare', which also means 'to explore'. In a space like the Tor network an individual has the power to accumulate mistakes and to embark on her own journey of personal growth and discovery, without fearing to incur in somebody else judgment (the simple awareness of this gaze would nip the exploration in the bud). In an environment configured to preserve the power to make mistakes, the error is transformed from an element to be sanctioned in one of truth: in the error lies truth, or at least the possibility of reaching it. In this sense, the idea of privacy conceived by Moritz is very similar to the one being traditionally developed in the West after the 18th century and characterized by a well defined structure of control and autonomy. Indeed, in his words privacy is a right being established to safeguard the inner sphere of the individual and her ability to challenge and contradict the authority and the tradition. Yet, although in this vision the individual is identified as the fundamental unit upon which society is built, privacy is not to be deemed at odds with social interests. On the contrary, the protection it provides from external intrusions serves purposes of public relevance (such as cultivating one's intellectual growth or enjoying without inhibitions one's freedom of expression).

When it comes to privacy, Astrid has a similar opinion. She is a former member of Tor Project and she is currently working for a civil rights association. She discovered Tor years ago, when, after her graduation, she moved abroad for professional reasons.

> "…after finishing the university I went to live abroad for a little while to teach English and I was blogging there, just to keep in touch with my family and my friends. That was the first time that I encountered Internet censorship because I used Livejournal to blog and that platform was blocked by the

> government. I never experienced that before. So I switched to Wordpress and I was connecting with bloggers there and all network there. And that's how I got involved in Tor".

Yet, her passion for freedom of expression has deeper roots and dates back to her adolescence. Born and raised in an environment characterized by, as she says, "pretty liberal vibes", since the years of her primary education she started to counter censorship and develop a critical mindset about it. The first allied that she had on her side was her mum.

> "Yeah, I do have a strong idea against censorship. This is because when I was a child my school library got the pressure of parents to censor books with sexual contents in them and my mother was really angry about it. I remember I got really angry with her and protest the school library. It did not actually work but it was a kind of first example that I think about for most of my life".

Political censorship and moral censorship: the eye of the beholder plays a conservative role that prevents the exploration of practices (or forms of knowledge) that are considered to be socially inappropriate. For this reason Astrid sees privacy as a reaction to escape the shame caused by such negative judgments. A reaction that, obviously, varies from context to context.

> "Astrid: I think that the reason we have privacy is because of shame, it is because the society we are living. So, for example, we have shame about sexual practices or about sexuality or about politics or whatever, and we need privacy to protect ourselves from those practices. So if you subtracted shame, you wouldn't necessarily need privacy. I guess from a conceptual philosophical level I am still conflicted how I feel about privacy, but in terms of the society we live in I think it is absolutely vital because of the fact we practice shame.
>
> Me: But, do you think privacy is a value itself or is a value enabling other values?

> Astrid: I think it is a reaction! I think that the need for privacy is a reaction. I mean, even on the most basic level, one of the thing that I find really interesting when I looked at privacy in our culture is the toilet… I know this is ridiculous but bear with me :) In the US you have toilet door to tear this part of your legs whereas in China you have open toilets with no doors at all. People have different level of shame when it comes to that particular habit. And so, privacy there is a reaction to shame. I mean, there are other things in different cultures that have other aspects of shame, but I see always them as a reaction"

Here privacy takes on the value of a cultural character (such as embarrassment in front of a fact considered socially execrable) being translated into the structure of the surrounding environment with the aim of facilitating (or constraining) the social action that takes place in it, as well as shaping it according to specific interests and values.

4.3. Escaping surveillance mechanisms

As mentioned in the introduction, the objective difficulty in defining privacy led several interviewees to explain this concept in negative terms, namely as something being opposite to surveillance. According to them, privacy can be broadly defined as a set of practices and knowledge that an individual (or a group) can employ to evade political or commercial surveillance. Interestingly, for some of the interviewees this specific idea of privacy results from personal circumstances that they have experienced long before putting their hands on a keyboard.

KM is certainly among those. Our meeting took place in September 2017 in one of the most iconic places for European digital counter-cultures, that is, the C-Base hacklab in Berlin. In a way, KM's story is typical – pretty much similar to that of the many hackers and hacktivists I had the chance to meet when I was working as journalist and researcher in Italy and in Great Britain.

> “Since I grew up, when I was 8 or 9, I have always been interested in computers. Growing up in a farm means you do not have the chance to meet your friends when you are young… Every time I could I went to online chat rooms, I talked to people, I could learn about everything I wanted. In Internet you are not judged by where you are from or how you look like or the age you are, and things can be discussed objectively”

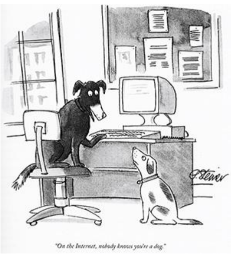

Fig. 13: Steiner's Internet dog

Geographical isolation, early interest in computers and a vision of the Internet that seems to closely recall the famous cartoon by Peter Steiner, published on the New Yorker edition of July 5, 1993. In this respective, KM regards privacy in a pretty traditional way, that is a socio-technical feature that provides individuals with an absolute freedom of expression without them running the risk of being exposed to discrimination or prejudice. Yet there is another element of KM's life that strongly influenced his hacking path – that is, his family background.

> “I guess my family is quite political. My father has a long history of left wing activism. He was involved with a political party for 25 years. He spent several years in prison as a political prisoner. So I guess, as I was growing up, I became left wing as well, interested in social justice issues and activism”.

As a matter of fact, this legacy affected his approach to technology. At the age of 16, KM began to be interested in hacking and offensive security. His first target was the website hackthissite.org (HTS). HTS defines itself as a "safe and legal training ground for hackers to test and expand their hacking skills"[6]. Actually, the portal is a simulator of hacking experiences, ranging from programming to computer forensics, from steganography to defacement. This kind of site is certainly not the only being present on the Internet, but there are a few specific elements that make it special. First of all, HTS was founded by Jeremy Hammond, a notorious name in the international hacktivist scene. In 2012 Hammond, an anarchist hacker and activist engaged in anti-capitalist and anti-militarist movements online and offline, was arrested and in 2013 he was sentenced to ten years. US authorities charged him for the involvement in the Antisec Operation, a political campaign carried out by the LulzSec collective (usually being considered as the

Anonymous technical elite group)[7]. The aim of the operation was to reveal the plot of relationships and connivance between US law enforcement agencies, intelligence corps and the Washington economic power. One of the main targets was Stratfor, a company responsible for the creation of a shady private intelligence network operating on a global scale. As KM explained to me, the political identity of HTS' founder has greatly affected the kind of challenges being proposed to the site users.

> "I guess that when I was 16 we did things like scripts challenges websites, which had different challenges like SQL injection and so on. 'Here is a page with SQL injection. If you got it, you will get some more points'. This is how most of this kind of sites worked but with HTS it was more political because of instead just having a page to hack, you had a whole story like: 'Here you have a Nazi site and you need to break in and find their membership database, take down their logo and so on'. This kind of services had a real political purpose…".

As anti-fascist and anti-capitalist militant, KM conceptualizes the privacy problem not so much on an individual level, and not even as something necessarily related to computer science, but rather as a condition required to resist the police practices enacted by state institutions in order to govern a territory and the population inhabiting it.

> "I grew up listening stories about the state detaining dudes and arresting people, having internment and all this kind of surveillance strategies used against people. And this is the history of how I got interested in how the state uses its power and how surveillance works. I think, I had the plug from my dad generation: the idea of confidentiality or privacy it is a very non-technical need of security. You see this kind of challenges, and they are the challenges of an activists group, and also having an understanding of computers and computers security and encryption and how encryption works… I've always seen this kind of stuffs as something for having independence".

KM's idea of privacy has little or nothing to do with the individual inner sphere. Not much because of his personal inclinations (he is sociable and open and he defines himself as a “a non-private person”), but mostly because his reflections about this problem arose within (and were shaped by) a collective political story (namely, that of his family and country). For him, the only confidentiality that matters is the one of the group because it make possible the communication between the individuals who are part of it and, therefore, their capability to organize and act. Without privacy, this possibility is not even given because individuals live their existence in an environment characterized by the so-called “chilling effect” – that particular form of inhibition for which an individual will never transgress the rules established by the watchman since she knows that she is constantly monitored and, hence, easily subject to sanctions.

> “I see it [privacy] as mean for people to help them to act independently or to organize together and get social activism [..] I see it as a collective value where people can feel comfortable in talking to each other, not to feel a fear (neither physical or subconscious) like they are being watched. I see privacy as a way of helping people to have collective action, to feel comfortable to be able to go where they want and work together. I see it as a collective benefit rather than a personal benefit”.

A similar concern is shared by the anonymous Tails developer ‘TD1’. The first time I met him was in 2018, during the Internet Freedom Festival in Valencia. I approached him because I needed a suggestion in order to help a friend in danger who was experiencing some issues with Tails. Without asking too many explanations, TD1 sat next to me in front of the monitor of my laptop to see what he could do to sort the problem out. I immediately got the impression that we spoke the same language, probably because TD1, besides being a computer scientist, is a militant in radical left-wing social movements (a connotation of his identity that he holds to remark strongly). When after a few months we spoke again, he did not tell me much about himself (nor I asked to be honest), but the location from which he was calling – an occupied house lost in the countryside, where a few hours later a self-organized rave party would have took place – was suggestive. According to TD1, since the very beginning of his experience as hacker and activist, there was no separation between politics, technology and organization. Between 2004 and 2005, he crossed for the first time the door of a hackerspace and he moved his first steps as hacktivist. At that time, he says, "people were getting organized on mailing lists and we were worried about what could happen if they were surveilled". For TD1, be an activist means to take part to a direct action, to hand out fliers, to call a demonstration, as well as to manage in a safe manner a digital platform being employed by a collective to organize this kind of activities.

> “…there was this whole issue about security: you prepare actions, you do some publications on line that may be your state does not like, or you want to organize stuff that you want to be secret until the last minute. And so, for us it was a direct concern, to be able to better control over our computing. It was a mean to protect ourselves from cops, police, undercover agents and so on. And also our communications, yeah”.

Either, KM and TD1 considers privacy as the capacity to bypass the surveillance mechanisms that regulate our societies. For this reason, they attribute a collective value to it, since they see it as a necessary mean to create organizational forms aimed at fueling social change. The invisibility before the eyes of power that privacy makes possible is a condition that both interviewees believe to be required for practicing activism. In other words, although privacy is not a transformative force itself, nonetheless here it is identified as a fundamental preconditions to challenge the rulers and leave open the possibility to produce a transformation of the present.

4.4. Privilege and social justice

While browsing the 2019 Tor Project’s homepage[8], one could feel like something is missing on the monitor. On the right-side section of the portal, under the heading “Who Uses Tor?", some of the typical users of the network are listed: journalists, military, police forces, activists, businessmen, IT professionals and ordinary people (labeled under the wording of "Family and Friends"). An internal page[9] provides further details about the ways Tor is used by individuals belonging to each of the aforementioned categories. For example, under the "Normal People" section one can read the words of users being worried at the idea of seeing their own online behavior being tracked by corporations and information brokers populating the advertising market; instead, the activism section refers to the several organizations – from human rights to environmental protection – that in the past have successfully used Tor to carry on their battles; finally, under the heading "Journalists", next to the names of international newspapers that use Tor-based whistle blowing platforms, the ideal figure of an information professional operating in a war zone – or in an area of the world subject to a tight surveillance regime – is mentioned. Yet, scrolling down the page, it is striking how very little space is reserved for marginalized persons and social groups, such as ethnic or religious minorities, LGBTQ people or migrants, who dwell outside of the typical presented "norm". I find this is a singular circumstance, since these individuals are usually strongly exposed to surveillance (and therefore, they are more in need of protection from it) either because of the prejudice they are object of and the disadvantaged socioeconomic conditions they experience.

I had the chance to talk about this issue with Alison Macrina, founder and director of the Library Freedom Project (LFP)[10], an organization aimed at educating US librarians to integrate privacy-oriented technologies in their daily job. On December 2015, when Tor launched its annual fundraising campaign, Alison was introduced to the broad Tor community with a blog post where she summarized the mission of her organization as follow: "Helping librarians understand privacy issues impacts not just libraries but the larger community [...] Libraries offer public Internet terminals, and librarians like me teach free computer classes to the public. Our patrons come from all walks of life, but we tend to serve communities particularly vulnerable to surveillance (including immigrants, Muslim Americans, people of color, people who are homeless, and those who have been incarcerated) in higher numbers than in the general population"[11]. Not surprisingly, this attention towards weakest and most vulnerable social categories has led her to take part (and to head until early 2019) the Tor's Community Team, namely a support infrastructure for users who are not tech-savvy but want to know more about Tor and to learn how to use it in a safe manner.

Alison is a radical left-wing activist engaged in many struggles. Initially, anti-fascism and mobilizations in solidarity with Palestine were the battles getting her major dedication but, over time she got engaged into more and more struggles. Political commitment is a second skin for her, something exuding from her daily life. Once that we had scheduled an interview, she arrived to the meeting a few minutes late. The reason of the delay, she told me while she was apologizing for making me wait, was due to the time she spent at the corner shop where she was discussing with her neighbors about an anti-fascist rally that would have took place in Philadelphia by the weekend. Also, before starting the recording, she introduced me her black cat 'Sabotage' – a name inspired by the famous Industrial Workers of the World logo – whose most favorite hobby was actually to sabotage her house. Alison's radical choices involve her life all-around, including her job. In 2009 she obtained a MA in Library and Information Science at the Drexel University and began to work as a librarian. She chose this occupation, she told me, because she was looking for a profession that "could have a positive impact on society, something for which I would have not hate myself for the rest of my life". While she was serving at the Watertown Free Public Library (MA), Edward Snowden brought to the light the revelations about the scope and the extent of NSA mass surveillance programs.

> "Intellectual freedom, privacy and open access are values which are directly related in the work of librarians. I was interested in privacy also before, but it was with Snowden that I realized how much these different values are connected and how there are deep connections between the loss of privacy and state components".

Alison was shocked[12] by the documents published by Gleen Greenwald on The Guardian and chose to fight back. She did so in an exquisite political manner, by taking action on the workplace. Initially, she organized computer privacy classes for the users of the library where she was working. Then, in 2014, she got in touch with the American Civil Liberties Union (ACLU) and she started to hold privacy workshops for other librarians. The initiative, involving 750 librarians and 15 libraries in three different states, has been designed by Alison with two goals in mind: first, to make her colleagues aware about the issues related to mass surveillance and, second, to teach them to protect the privacy of the users they worked with. In 2015, she started her collaboration with Tor and received a grant from the Knight Foundation New Challenge, in order to expand her privacy advocacy work on a national scale and turn it into a full-time job.

In her own view, privacy has not much to deal with domestic intimacy or extension of private property but it is a word that she associates with an idea of control:

> "...privacy is control and I think of it in this way because I tried to think about it in terms of power relationships and power structures. For me, privacy is strictly related to control. Particularly, it is related to the idea of personal autonomy – I hesitate to say freedom because it is something which has been corrupted with bourgeois bullshit too – that is to say the ability to make a decision about the self".

Although the right to privacy is recognized on a juridical and formal level, Alison believes that its exercise is given within well-defined power structures that constrain the actual possibility of individuals to enjoy it on a material level. A possibility that, in Alison's experience, seems to be denied to the most unprivileged categories of the US society.

> "When I work with people from those different groups, marginalized people I mean, one of the things that I heard most is "Where the fuck have you been? This has been happening to us forever". Black people in the US have never had privacy. When we abducted them from Africa until now, we have used the state to fight and monitor them. So when you tell them "Download this thing for your phone" the answer usually is "Get fucked, there are surveillance camera on my house". It is a daily thing for them engaging with the state surveillance which, mostly, affect marginalized people".

However, according to Alison, it is not only a disadvantaged social condition that makes it difficult, if not impossible, to exercise the right to privacy. Another obstacle of cultural relevance being denounced by the activist is the underlying elitism affecting the FLOSS movement. In her view, there is a kind of partitioning wall between tools aimed to protect privacy and the subjects that could benefit the most from their adoption. The bricks that make this wall are essentially two: the jargon geek being used by many hackers – a language that Alison considers exclusionary and exclusively aimed at raising the social status of those who employ it – and, above all, a hyper-individualist and pseudo-libertarian attitude that it is shared by many open source developers. A problem whose meaning is summarized by Alison in this anecdote:

> “I used to live in Boston and Richard Stallman lives right near there and I see him all the time. And one time I was somewhere he was and I had this huge fight with him. He stated that he would never recommend non free software to anyone, even if it was a serious situation. He just could not conceptualize that there are basic material needs that people do not have met, and free software is not going to meet them. The hypothetical example that I gave him is: “I work in the library and some come in and say ‘I have a job interview in an hour. Can you teach me how to get on Skype?’” Stallman was like “I would not teach this to them. I would tell them that their freedom is more important”. And my answer was “What do you know about people freedom?”.

Here the possibility of enjoying the right to privacy is not only limited by class membership or by the “line of color”, but also by the elitism of the FLOSS movement, exemplified by Stallman’s words. Indeed, the Free Software founding father seems to think that freedoms originating from the openness of source code are the only ones that a human being has the moral duty to aspire to. The existence of other conditions (such as social belonging or material needs), that precede such freedoms and in fact make it impossible to enjoy them, is not even took into account. According to Alison, the translation of this cultural character into encryption software produces exclusionary access criteria that transform the right to privacy into a privilege for the chosen few who can afford it. Another way of thinking it: a privacy software being designed by an engineer with an audience of engineers in mind will end up being used only by a relatively small population, namely by those subjects who already have enough technological resources or social capital to bypass the surveillance *dispositif* in many other ways. The result is paradoxical: those who are less exposed to surveillance become the main users of encryption, while those who are actually in danger are unable to use it.

> "I do not think that free software is on its own radical. I think it has radical potential, but I think that it is entirely dependent on how much we will focus on engaging with those kind of power structures and we have not done it. We really have not done it".

In other words, within the power structures denounced by Alison, the emancipatory potential of these instruments simply does not arise. A problem that, on the contrary, is strongly considered by librarians involved in the defense of privacy:

> "I love working with librarians, because even if they are not on the precise part of the political spectrum that I want them (there are lot of leftists in libraries but most of them are liberal) they engage with the most different kind of public everyday and they understand what the material realities are to those people. And this is something which is not really present in free software at all".

Although her way of understanding privacy is quite traditional (namely, a form of protection of individual autonomy), Alison developed an interesting point of view on this matter. In fact, her dual role of librarian and political militant led her to identify the material and cultural limits that circumscribe the concept of privacy and the possibility of enjoying it, as well as the power structures from which these boundaries originate. At the same time, she suggests to deal with such power structures and to develop strategies so that the privacy ensured by a technological infrastructure is no longer a privilege for a few, a status quo that a handful of geeks can boast about, but a right for anyone, including the most marginal social categories.

4.5. Daily routine

When you are interested in infrastructure (and this applies for privacy-oriented infrastructure as well) it is difficult not to feel a shiver up your spine when it happens to meet an engineer talking about routine, habits or even boredom. I vividly remember to have experienced this feeling for the first time when, at the end of 2014, it happened to me to stumble upon a post published on the Guardian Project (GP) blog being titled

"2015 is the Year of Bore-Sec"[13]. GP is a notorious team of hackers in the US and European scene, particularly known for the realization of a Tor porting for ARM processors ad Android smartphones. The article in question was a call for gathering ideas on how to embody into mobile devices an idea of security “so easy and seamless, that is boring”. And it added: “This is no longer about James Bond super-spy technologies, it is about having as little impact on your day-to-day use of mobile technology while still providing the maximum protection to your data and communications, as possible”. In order to make the concept clearer, the post was accompanied by images which depicted some past invention from which GP claimed to draw inspiration in its hacking activity: a smoke detector, a speed bump, a life jacket, a lifesaving outlet. “We want our code to be as much as boring”, the hackers wrote. The imaginary leap they proposed was so radical for me to be alienating. Indeed, at the time I was more familiar with other hacker cultures (such as Anonymous) who declined the concept of security according to an attack/defense logic: in my mind Tor was a tool for planning an action, or a protest rather than a daily communication network. I associated this technology with an extraordinary dimension: epic, salient, clandestine, secret and, therefore, exciting, but nonetheless extemporaneous.

GP’s approach was completely different. For them it was no more a matter of wielding a tool against an opponent in order to damage him: on the contrary, they wanted to invent so convenient and user-friendly technologies that the majority of common people would have asked to wield in order to conduct their daily life. Here, the goal was not about actively using a security device for achieving a specific political agenda. On the contrary, here the political agenda was engineered within the technical tool, embodied in its same form and conceived as one of the functionalities being coded into its design. The politicity of this rationale lies in the fact that, once taken in hand, such technologies would have shaped the physical and social life of the millions of people resorting to them, by regulating and conforming their daily behaviors, without them even noticing. Nothing more exciting than this "boring" approach to security that, with its invisibility, questioned the nature of contemporary power that, to say it in the words of the Invisible Committee (2014, 152), "is the very organization of this world, this world modeled, configured, *designed*", ruled by "an order that embodied itself in the objects of everyday life".

And precisely “everyday life” is the expression that best sums up the idea that I got of Nathanial Freitas (GP leader and spokesperson) after having spent a couple of afternoons in his company in the summer of 2019. For those having had the chance to make his acquaintance, it might sound weird to associate his personality with the idea of routine. After all Nathan is a public figure, being especially known as a seasoned activist. As he told me, the credentials and the experience that he got in the context of the environmental and human rights struggles actually facilitated his earlier contacts and opinion exchanges with Tor Project in 2009. Yet, at the same time, the way he told his story – very open and without sparing any details – gave me the impression that his relation with digital technologies, his choice to embrace the FLOSS philosophy and fully dedicating himself to online privacy, security and anonymity – these are such important aspects of his life that he does not hesitate to label them as "existential" ones – were actually the result of a set of mundane experiences, somehow trivial in their way, occurred on the workplace, in the noisy family routine or even while practicing his religious creed. And, of course, during his childhood.

Not even ten years old, Nathan is already a coder. On YouTube it is possible to find a recording, probably dating back to the early '80s, starring him as its protagonist. He is attending a TV show and, with a slightly know-it-all attitude, he is talking about string variables and programming to a presenter who looks visibly uncomfortable because of his scarce familiarity with the topic. I instinctively felt antipathy towards that adorable scoundrel that, so young, already mastered the commands of an Apple with the ease of a seasoned engineer. "A predestined" I thought. "Is it because of his social class?" Not really. Nathan’s roots are, in his words, "very humble" and he is very proud of them. At the beginning of the 20th century his grandfather arrives in the US from Portugal and, after unlawfully crossing the borders, he becomes a peasant in Northern California. A life of sacrifices allows Nathan's family to climb some steps of the American social ladder. His father becomes an IT employee for the State of California and conveys his passion for computer science to the son. Yet his first computer is a present from his mom, a teacher at a local high school that managed to "kind of smuggle" a machine for Nathan from the institute she was working in. The '80s California context affects, and somehow facilitates, his inclination towards hacking. At that time, he tells me, the Silicon Valley was not that technological and financial center of power that we know today.

> “It was that age where the distance between the Silicon Valley and the rest of the people of the State was not so far. These were small companies with new people that worked on Commodore and Apple… and, you know, Apple gave my school computers, and they were fixing Apple II and we had the ability to have them and we did not need to pay a lot of money, cause… I mean we were near Apple, like only a hour away”.

As it was inevitable for a golden boy of coding grown in the global epicenter of the computer revolution, Nathanial finds a job in the ICT sector and in a short time he manages to carve himself a prestigious position in the mobile industry. In 1998 he goes to New York and starts to work as lead developer in the ‘creativity division’ of CTNY, a company specialized in web-based applications, e-commerce, enterprise integration and messaging websites. He mostly develop Java language applications for the distributed web. In 1999 he leaves the company and establishes with Jon Oakes and other former CTNY colleagues ThinAirApps, one of the very first companies to develop software for the nascent mobile industry. At that time Google was little more than a startup company founded by a couple of former Stanford students, Jobs had been back in Cupertino two years earlier in order to help Apple to leave behind a long period of financial woes and Microsoft was getting ready for the launch of Windows ME after the global success of Windows 98. Android, iOS or Windows Phone were not even experimental prototypes and the future had the form of BlackBerry, Newton or Palm devices, at that time being called PDA (acronym for Personal Digital Assistant). ThinAirMail[14] was the most successful software developed by Nathan’s company: a security and usability-oriented email client – that still today he refers to with some pride – and that in a short time drew the attention of Palm.

> “It was between 1999 and 2001. Palm needed a competitor to the Blackberry, and Blackberry had an encrypted end-to-end thing for the enterprise. And

> we had our own server for the enterprise and we implemented a cross platform encrypted messaging stack. The keys were managed on the server because it was an enterprise product. So it was not like, let's say Signal with decentralized key storage, but it was really innovative, very powerful…".

ThinAirApps is bought by the US corporation in 2001. It is a first turning point in Nathan's life: a series of events will originate from this acquisition, eventually prompting him to entirely embrace the FLOSS philosophy. In that period, the bulk of his earnings comes from the integration of ThinAirMail into Palm devices and not from the royalties on the software. "Licensing is not a great business unless you do not have a unique position" he tells me "We were just getting a nickel or few pennies per device". To be fair, the thing is not a great concern to him. Even back then Nathan does not consider technology "as a way for making wealthy people wealthier", but as a force for giving more power to common people. He can rely on a good income and – far more important for him – he know that he is developing an innovative technology which can improve the life of the people using it. In short, things are going great. Yet, suddenly, the table turns and Nathan realizes that having sold to a private company the intellectual property of the his code is a mistake that he cannot amend. In 2004, without giving any further explanation, Palm decides to put in a locked file drawer all the patents bought from ThinAirApps and to stop to implement the software into its enterprise devices. For the Californian hacker it is a shock.

> "… one day Palm decided: 'Oh, we do not want do this anymore, we do not want be in the enterprise anymore' and they just got rid of my team and said: 'We will keep you in the webOS'. I was just so frustrated that I put so many years of my life building something that I thought it was important and this corporation basically said: 'We are not doing this anymore. We control it and you are not going to see this code again'. And so I thought: 'I can't waste these essential years of my life for something that it is not going to be lasting'. That's how the open source came in. I never wanted to do something again that could just be thrown in a dusty shelf, or in the trash or lost".

Yet, in the meantime other events happen in Nath's life, giving a swift turning point to it, almost a derailment from the safe binaries where it seemed to be settled. 9/11 befalls America with the same violence with which the 175 flight of United Airlines crashes on the glass and steel facade of the Northern Tower in Manhattan. Nathan first witnesses the terrorist attacks orchestrated by Al Qaeda, then those carried on by the Bush administration in the name of the fight against terrorism. Along with dozen of thousands of innocent civilians from New York to Kabul, the “Enduring Freedom” operation targets also a number of political and civil freedoms which American citizens had been enjoyed for generations. With the Patriot Act, the constitution of the country comes under attack. Domestic surveillance – something that in its electronic form was already intrinsically possible because of the buggy design of the IP – spreads quickly and unchecked.

> “Obviously a critical moment in the US was 9/11. I was in an office at work in lower Manhattan, I saw the plane hits. It was very personal incident for me, and I became very frustrated with our country response, and then the move to surveillance, the Patriot Act and all the things that followed. I already knew that it was technically possible and I saw the government moving towards that direction. I saw this not being in line with our Constitution and so I wanted to get rid of it and I started working on things like what we have done with GP”.

Actually, towards the end of the ‘90s Nathan had already had an earlier turn towards activism. His job at the upper echelons of the mobile industry brought him in contact with military representatives and big pharmaceutical companies contractors, making him feel “less positive about the work I was doing”. For this reason, he chooses to get involved on the front of environmental and human rights protection. He does that, *ça va sans dire*, in the most suitable way for him, that is, bringing his technical skills and knowledge of the Internet to the activist groups with whom he cooperates.

> “In like the late 90’s and early 2000’s I’ve started doing activism kind of moonlighting, where I would go working with an activist group in New York and I said: “I think you guys need some BlackBerry” and I would configure them a bunch of devices, teach them how to use them and I would help them

> to secure their mail systems and did that just as a volunteer. But more I became involved, the more I said "wow, the human rights and environmental groups could really benefit from more expertise" around communication technology. So, I got pulled in, more and more and more and I became so less interested in the customers that I was serving in my day job".

Yet, when I ask him which events influenced the most his idea of privacy and what he refers to with this concept, Nathan gives me an answer that does not refer to his struggle for human rights but to his religious creed. He belongs to the Unitarian Universal Church, a sort of liberal religion being opened to all other professions of faith which pursues the achievement of equality and social justice ideals, in addition to a spiritual growth of its community. To make an example, the universalist associations work a lot with migrants who arrive in the United States: their members are actively engaged in facilitating their integration and they struggle in order to make political authorities to recognize and to respect their rights. This activity has never been easy, yet today has become even more dangerous, because of the mass hysteria triggered around the matter by the Trump administration and the pervasiveness of the US domestic surveillance system. In order to reduce the risks resulting from an unwanted exposure to the eyes of intelligence agencies or those of the Immigration and Custom Enforcement (ICE), the hacker decides to teach the ministers of his cult how to use Signal. In order to make it easier to understand the goals for which the tool was designed, he borrows a metaphor from the 2015 UN's report on privacy and surveillance which results immediately clear to men of faith.

> "I was trying to figure out how to talk about Signal and I got this idea from the David Kaye's report published few years ago. He is the UN special rapporteur on surveillance and privacy. In his work he mentioned "dignity" like in a very personal way. So, I said this to my minister: when someone comes to you and has a very personal issue to talk their religious leader about, that's a private conversation, that's a very personal private thing… That's something that should exist in a digital form, a level of dignity or

> confidentiality, in a very caring way that you feel you have this channel unable to be violated".

Yet, Nathan feels compelled to preserve this same level of dignity in other digital spaces as well, like, for instance, the one that overlaps and informs the most inner sphere of domestic affections. Some years ago n8fr8 (one of the nicknames he uses online) *forked*[15]. Or, to say it in a more traditional way, he became a father. Inevitably, this experience deeply changed his perspective about the world, also from a technological perspective. A trivial tool such as a smartphone ends up assuming new meanings along with those ones that the hacker had previously ascribed to it. Unlike before, he does not use an Android device or an iPhone only to organize a mobilization or a political protest but also for taking care of his new family day-to-day. And even if the context changes (or rather, a new one joins the former, stratifying and melting with it) the need to securely communicate does not fail. Indeed, the devices he and his wife use in order to keep in touch are properly set up to prevent that the privacy of their children – and therefore their dignity – can be violated.

> "This is also a funny angle on it, which is: as a parent, your kids will get rush on their skin. My wife would often take a picture of my daughter's body and send such picture to me. And it will send such picture to our pediatrician and ask her "Should we go to the hospital?". One time she sent a picture to our friend and she told us: "Go right now to the urgent care, that's a very bad infection, she needs to go immediately". And the idea that we were texting pictures revealing part of my daughter's body… We should be able to do this, but we should be able to maintain the dignity and the privacy of my daughter and also protect us from being seen as criminals sharing nudes pictures of children".

The arrival of a child is a happy complication for Nathan who finds himself crossing from a context to another (his family, his work as engineer and his activism) where he plays different roles. This situation drives him to develop technologies that enable him not only to appropriately face the different threats involving his informative sphere but also to ensure that such contexts are adequately insulated – in order to prevent an accidental leak of information across them with unpredictable consequences.

> “When you use children photos, you want something which is very reliable. As an activist, it is also interesting when my kids grab my phone and all the media... When I took the photo of ‘Black Lives Matter’ protest, with people being arrested or someone being beaten up and my daughter trying to look for picture of her swimming at the beach, she sees these photos and see all the photos on my phone and I have different lives and I want some photos to be secure over here and some other not, and I do not want Google mixing a picture of an activist with FaceID, with my family.. It is so problematic when your life is a little bit complicated...”.

This real life example clearly shows how the concept of leak is neither exclusively pertaining to Julian Assange, nor it refers only to the breach of diplomatic databases or to precious industrial secrets. On the contrary, it is a very common condition that potentially affects anyone being connected to a hypercomplex network like the Internet. Yet, there are other threats Nathan is worried about, dangers that technological mundanity reserves to contemporary societies whose scope extends well beyond the indiscriminate leak of a set of personal information. Internet is a giant with clay feet ("its fundamental components" he tells me "are essentially broken"), whose fragility is further worsened by the fact that the web is based on poorly implemented critical infrastructures (he particularly refers to the electric grid) which, in turn, rely on the Internet itself in order to function. This short circuit of vulnerability is made even more dangerous by politicians that prefers to keep themselves at a distance and not to fix it: promising that an infrastructure will work as expected does not ensure electoral consent since everybody just take it for granted. Infrastructural maintenance does not match the sensationalism criteria required by the generalist mainstream media, nor it allows a candidate to cut a ribbon with giant scissors in front of an audience of photographers, cameramen and reporters.

Yet the problem is that, when the wind of casuality starts to blow in this pinwheel made of technical vulnerabilities and political shortsightedness, then its rotational movement risks to become unstoppable and to turn its spiral into the eye of a cyclone with potentially devastating effects. Like it happened for instance in August 2003, when a software bug in one of the ‘FirstEnergy’ electric company control centers caused a cascading blackout which affected Ontario and the US East Coast northern states. For two weeks, in two different countries, 55 millions of people were let in the dark, or could enjoy electricity only for few hours per day. Nathan was among those. He does not hesitate to define that event a "turning point”, that lead him to develop other reflections still affecting his approach to coding and privacy.

> “After 9/11 I was worried. When the 2003 blackout happened, I thought ‘here we go again, they have taken down the grid’. The reality was different and after that I got pissed off. We keep talking about war, terrorism, cyberwar and all these things, while ignoring our critical infrastructures. Do not get me wrong, please. I am sad when somebody is killed by a terrorist attack but the number of people killed by other means around us is definitely much higher. What I am really worried about are the stuffs around us in our day to day life. This is our planet, our country and our towns. We need to solve this and encryption is really crucial in this perspective: it should not be something just for banking but for every aspect of our life. We, as GP, want encryption to be the norm everywhere and the idea of protecting metadata for us is key”.

Through the years, GP put many efforts in increasing the security of a growing number of daily objects being connected to the Internet. The list of the projects carried on by the group is very long. Phone hardening[16], security patches for the Mozilla code, the encrypted database SQLcipher[17] (widely being used both in the Android and iOS ecosystems). And along with all this, it is worth mentioning a continuous technological experimentation carried out so that the daily chatter, the exploration of new ideas and the research of information for study purposes can remain what they actually are: that is, *ephemeral activities* and not, he tells me, “a permanent thing” bound to perpetually mark the existence of an individual. Finally, the implementation and usage of onion services in the most common daily scenarios, in order to protect data traffic from wiretapping and passive surveillance. Some of the applications he conceived fall under the scope of the so-called Internet of Things and affect the sphere of domotic (here Nathan worked on the Home Assistant project[18]) and surveillance of physical spaces (like for example the Haven app[19], sponsored by Edward Snowden). Other projects are linked to self-hosted platforms of cloud computing (like Nextcloud) and to the creation of a safe system for online backup via Tor. Still others deal with file sharing or use of apps for online dating (like Grinder) in contexts where homosexuality is severely punished. Last but not least, Nathan advocates the use of onion services to reduce the attack surface of critical infrastructures as well (such as those for smart cities data collection or for power plants administration).

> "Two or three summers ago I did this thing of the Onion Internet of Things and I built Tor into a couple of open source Iot platforms. I ended up going to the Army Cyber Institute at West Point military academy, here in NYC, to give a talk. They invited Tor, Cory Doctrow and all sort of people. And for me it was a really great audience to say: "Hey look, you are tasked in defending critical infrastructures, here is all the weaknesses and at the same time we have things like Tor that are invented by someone in the NRL and you are not even taking advantage of it because of fears of… because of surveillance really. I told them that every power utility should be connected only over onion and, more precisely, over stealth authenticated onions".

Nothing more boring than this. All in all, as Nathan remarks at the end of our chat, "for me using Tor is the equivalent to sit at my table and reading a newspaper".

4.6. Beyond privacy

From the data I gathered another significant attitude towards the issue of privacy emerged. In fact, many of the hackers and activists I interviewed not only had an objective difficulty in defining such a foggy concept; but they went even further, by challenging its political usefulness and by suggesting its replacement with other terms and conceptual schemes. The first person who came up with this kind of reasoning was

Nix. Born and raised as a hacker in the underground scene of his country, Nix began to deal with concepts such as "hacking", "wiretapping", "hijacking", "attack" and "defense" in the late 90s, when these terms had not yet been codified into a vocabulary, but they were object of practical experimentation carried out by niches of geeks and enthusiasts. In this cultural and technological *milieu*, Nix learns to use cryptography in order to protect his communications. Understanding these techniques and putting them into practice immediately leads him to wonder what the relationship between technology and politics is and how to produce a societal impact through his hacking process: "Cryptography is cool" he told me during a chat session "it is something you can do because it is a power at your disposal". However, at the time it was not clear yet what purpose this power should had, nor how it should be used:

> "It was '97 or '98, I do not recall exactly, and there was this theoretical debate about what hackers were supposed to do. Were we supposed to do politics or to create technologies? My first impression was that in the technology we were using there was no political imprinting, unless somebody openly declared it. Then, my provocation, my incitement was "Do we really want to do something political? Let's use PGP!". I realized that it was not enough to create a tool for protecting my communications, something used by me and a couple of dudes. I mean... until that moment I was not interested that my software had an impact: I was just interested that my software worked for me".

Only later on Nix will understand that these technologies represent instruments for exercising a power. When this happens, it is because he himself has become a target of such power. In early 2000s he worked for an IT security company and he was the only employee in the staff featuring hacking skills. His boss did not trust him and began to monitor and wiretap (actually without success) his Internet traffic on the workplace.

> "I do not know why they had to wiretap me, without any kind of actionable facts. It was a demonstration of a possibility, of a power for its own sake. I got pissed off by that lacking of trust. From that moment on, I started to associate several facts: this lacking of trust, the shady security company I

> was working for, the fact that they tried to wiretap me, the fact that I could protect myself, the fact that they would not deserve my trust, the fact that they were not able to interact with their employees (we were just a few)".

After a while the professional relationship with his employers ended, and not without further disagreements: indeed, Nix decided to write a few backdoors and to hide them in the infrastructure of the company he was working for. "They were very theoretical objects" he claims "not only because it would have been very difficult to detect them, but also because it would have actually been been very difficult to use them". Nowadays Nix expresses a very negative opinion for what he did then: not much because of moral reasons, but for the weak effectiveness and the poor result of his reaction. His only repentance is that he did not create any real damage to his former employers.

> "What is the point of writing a backdoor if you are not going to use it, or if you do not protest the human resource management, or if you do not understand the situation which had determined such issues? I think that my reaction was just a way to feel 'smarter', something to heal my maladjustment. It was a way to suppress an emotional outburst and, at the same time, to create solutions which were working just in my mind, without these being actually producing any true impact. It was just a technological form of betrayal, something that I considered as a form of power through which I was reacting to another form of power."

This experience lead him to become a privacy advocate: his main interest was to deploy an ever-increasing number of security features in mainstream technologies being used by ordinary people. Yet, as he explained to me, the concept of privacy seems to fascinate him very little. "I cannot even define it". Nix openly acknowledges that metadata and content in our era have a huge economic value and, as his experience suggests, "they are power carriers". Therefore, in principle, privacy could be associated with "a doctrine that explains why it is necessary to protect data, have control over them and be able to claim rights regarding their use". Yet, he is aware that such concept is situated in a semantic field being crossed by opposing tensions:

> "[Privacy] is that particular word which is usually associated with a second signature for official documents. Otherwise, if you take care of your privacy you are usually seen as a dissident and if you are a good citizen you do not need to take care of it. I think privacy is a word which is an ideological conglomeration of hypotheses made by a person without being properly informed about it".

Whether it is a bureaucratic quibble or a suspicious attitude, Nix realizes that, in the eyes of a random user, privacy is essentially seen as a limitation, a burden, but definitely not as a mean of empowerment. In order to explain this point of view, he uses an analogy:

> "In the ICT security corporate world, if you find a bug in a software then you have created a problem: it is your fault. Instead, if you find the solution, you are a superstar. When I was working for a major firm, and somebody found a bug, they never reported it to the management. They just anonymously published it in full disclosure so that they were able to provide a solution for the company without creating a problem. Hence, these kind of experience I had in the past made me think: 'I cannot go to a person, who presumably has already her problems and create her another one' – that is to say, privacy".

Nix has decided to wipe out the word 'privacy' from his hacker and activist vocabulary: associating a technology with a concept normally perceived as a hindrance to online daily activities, or which can be a reason for unwanted attentions (and even troubles with the law), certainly does not favor its mass adoption. For this reason, he decided to replace this abstract and equivocal notion with conceptual frameworks capable of emphasizing the actual benefits resulting from the use of a privacy-oriented infrastructure.

Does Tor provide privacy? No, but it allows to enjoy a "full freedom of expression" without being subject to undue interference. Do onions provide privacy? Not at all, yet their use allows to benefit of a "free, independent and reliable personal data management". Does Tor Browser provide protection from surveillance? You will not hear the answer to this question in the seminars held by Nix, because the term ‘surveillance’ (one being deemed no less vague than ‘privacy’) has been expunged from his vocabulary. The hacker rather prefers to talk about the active role of algorithms in modifying the way that we perceive information when browsing a social media and how to take back the freedom to look for the information we really need: in this perspective, Tor Browser is a tool to take care of our “digital hygiene” (or, alternatively, to maintain a strict and healthy “information diet”). These lexical changes are not only made to prevent the emergence of any psychological pressure in the user – the typical feeling that leads her to say “I have nothing to hide, hence I am not going to use any PET” –, but also to engender in her a sense of empowerment, something which can allude to a real and practical improvement of her daily condition.

This reasoning echoes TD2’s words. TD2 is an anonymous Tails developer who I have met several times during hacker conferences and meetings. He is a long-time hacker with a strong left-wing political inclination, even though he is hesitant when it comes to stick to a predefined political label. When he speaks about himself, he asserts to care about "how power is distributed, how resources are shared and distributed, how we relate each other and what is around us". TD2 is extremely careful in managing his real identity. Although in a couple of occasions I had the opportunity to talk with him for a few hours, I do not know his real name. For a long time, I was not even sure about his origin. Yet, despite this attitude, when we met for a brief interview, TD2 immediately showed to be not particularly keen about the idea of privacy. When I asked him what he means when he refers to this concept, his answer was quite straight: "I do not know, I do not use this word too much".

> “Privacy is focused on the individual and for me what matters more is what I share with whom. It is not about: ‘Hey, there are some part of me of my life that are strictly me and nothing else, it is just my personal and individual life’. This is not the way I think of myself. My first concern is that of being in a position to express consent about what I consider to be part of my intimacy; whom I want to share part of my intimacy with; what I do not consider intimate, but, still I do not want to be public on the Internet and visible to

> everybody. Rather than thinking in terms of privacy, I try to think more in terms of consent and sharing".

TD2's skepticism about privacy is not only due to the historical bourgeois origins of this concept. In his own view, privacy, with its blatantly individualistic features, is just inadequate to ensure the protection of users' data in the complex network of social relations mediated by the Internet. As a part of this, the hacker points his finger to the indefiniteness of the term: "It is simply too blurry and nobody really knows what it means". Also because of this reason, when he holds a workshop for introducing new users to the Tails' principles and goals, he carefully avoids any reference to this word.

> "Last time I gave a talk about Tails, I approached the theme in a total different way. I said that my job is trying to make computers behave the way we can legitimately expect they should behave. If I want to delete a file, I expect it to be deleted. If I click the 'Delete' menu option, I expect it delete a file. If I type 'nytimes.com' on the browser address bar, I expect my computer to create a connection to the web server that hosts the New York Times site. I do not expect it to be fully peer-to-peer, but I am still expecting that I am connecting from my computer to that one. Certainly, I do not expect that twenty more computers will track me by recording which page I am visiting and from which page I am coming. When I try to explain what I do [as Tails developer], I say that I try to make what is hidden – what you do not see as user – working as expected, without you need any knowledge of computers. I also try to explain that I consider my geographical position as part of my intimacy: I want to be able to choose whom I am intimate with and I might not want to be intimate with Google."

TD2's goal is therefore to create an OS that does not betray user expectations about what is public and what is private: a Tails user must be able to fully rely on it, she must be reasonably sure that it is designed to do nothing but what it promises. Not only the graphical interface has to be intuitive but its has not be equivocal or misleading by any mean. When a user digits a command on the keyboard or clicks the mouse pointer on the monitor, Tails has only to produce the effect she desires: nothing more (like moving a deleted file to a sub-folder, and removing it permanently only after a period of time being arbitrarily established by the OS manufacturer), nothing less (like deleting a file without overwriting the disk, thus making it possible to recover it). The same should happen for the network protocols being employed by a device in order to transmit information over the Internet: only the data that a user wants to share has to be transferred, and only to the legitimate recipients she decides to share such data with.

The inherent complexity and limitations of the concept of privacy clearly emerged from Arturo Filastò's words as well. Although being very young, over the years Arturo (also known under the nickname 'hellais') has carved out very significant roles in the Tor community and he has taken part in the creation of some of the most relevant projects which have emerged from it. Among the founders of Globaleaks, Arturo is also the creator of the Open Observatory of Network Interference (OONI) and lead developer of OONI Probe. As he explains me, since day one OONI's goal has been two-fold: on the one hand to standardize a methodology for measuring online censorship; on the other, to provide a scientific evidence – that is, data sets built with verifiable methodologies – for fueling political initiatives against it.

> "Until few years ago we had only a few poorly written scripts and commands for measuring and detecting censorship. We used these tools to investigate various cases of Internet censorship that Tor users from several countries reported to us. At that time, there were already several initiatives being aimed at mapping censorship on global scale. However, we were a little dissatisfied with the lack of data and technical information no how this kind of research was conducted. They usually told you things like 'the level of censorship in country X is high/medium/low'. These parameters were pretty sloppy, though: it was not clear what they meant, nor what their value was. Moreover one had no access to the tools which had been used to make that measurement and, hence, it was not possible to evaluate their accuracy in technical terms. Finally, since nobody had access to the methodology that was used to generate those measurements, it was not possible to build on past results."

In order to overcome these limits Arturo developed OONI Probe, a cross-platform censorship measurement toolkit available for desktop and mobile (it runs on Android, iOS, Windows, Linux and Mac OSX). Initially released in 2011, OONI Probe is an application designed for detecting and identifying any technical measures being arbitrarily deployed by an ISP in order to filter or manipulate users' traffic. Run by thousands of people scattered all around the world, OONI "has collected millions of high quality measurements from nearly 200 countries using open methodologies, using FLOSS to share observations and data about the kind, methods and amount of surveillance and censorship in the world". These data are used as the raw base for periodic public reports about the state of online censorship in many areas of the world, with a particular focus on the Global South.

There is no need to say that transparency is a crucial value either in Arturo's ethics and OONI's vision. In his view, the Internet transparency and the accountability of the administrative procedures governing it are the minimum required coditions for the network to remain democratic. The organization hellais belongs to does not contest in principle that information may be regulated by a political authority – to the point that OONI representatives have always taken public stance by claiming that phenomena such as online child pornography should be severely fought. Rather, they oppose the fact that this kind regulation is almost always imposed without the citizens being able to express their opinion about it and that, above all, it is implemented in an opaque manner. Indeed, when an ISP makes a content not accessible behind a court order, it hardly makes this operation explicit to users, but rather it prefers to simulate a fault of the site that provides it. The opacity of the censorship therefore lies in its dissimulation character, in its attempt to disguise itself as a technical malfunction which actually conceals a political will. Hidden behind this mechanism, a government can resort to censorship in order to define the boundaries of a communication system and to establish which topics can be legitimately treated within it (and which ones should instead be excluded because of their 'inappropriateness'). OONI acts to overturn this dynamic and to reveal the existence of censorship systems to the public, to make them transparent, to bring them out of the technical fiction within which they are concealed, to represent them, to give them a shape and, ultimately, to fuel an informed debate about their actual legitimacy.

In this perspective, OONI can be essentially considered as a space of action and information for keeping the Internet ‘open’. Yet, this adjective must not be understood as a mere synonym of ‘easy-to-surf’ or ‘hard-to-censor’. Here, the idea of ‘Open Internet’ has to do with that one of a communication medium which can be understood even by an ordinary person and embeds a concept of public accountability for those in power.

Given the central role that transparency plays in OONI’s philosophy, I was not surprised that, when asked about privacy, hellais shared with me an interesting reflection about the contentious relationship between these two concepts. "I think that sooner or later" he told me "we will need to stop talking about privacy and get rid of it". Obviously, Arturo does not want to give up on the confidentiality of his communications, nor on the control over his data. Simply, with this statement he wants to emphasize that nowadays privacy presents two problems which make it mostly useless. First, it is a polysemic concept,

> "a term characterized by so many nuances of meaning, often very different from one another, that it is difficult to understand what one is talking about”.

Second, privacy is generally seen as something being opposed to transparency and at odds with it. However, in his own view, the two terms are not to be considered mutually exclusive. On the contrary, it is necessary to find a balance between them, "a sense of compromise between the individual right to privacy and an oversight of the processes that affect society". In his opinion, it is simplistic to think the problem in term of the most famous Wikileaks’ slogan (namely “Privacy for the individual and transparency for corporations and public institutions”) because "individuals work in corporations and institutions. So, how can we know that things are happening in the right way, I mean without being tainted by corruption dynamics, and at the same time protecting certain information that must not be revealed to the public?". This dichotomy between privacy and transparency is a problem that Arturo had to deal with during the early development of Globaleaks.

> “If you think about it, a platform like Globaleaks is designed in order to bring transparency. Also, it has to protect the privacy of a whistleblower. Yet, at the same time, as a founder I felt that I had the duty to avoid that it could

> be abused in order to violate someone else’s privacy as well. Globaleaks was designed in order to be a confidential communication channel for transmitting information from a source to a recipient (a journalist, a public body or a private company) and not for making them immediately public. The aim of this design is to avoid problems linked to abuse: for instance somebody who tries to use a whistleblowing platform in order to gather information on a minority and make their personal data public”.

This irreducible tension between privacy and other values emerged in other interviews as well. For instance, according to Nix, there is a more and more evident dichotomy between privacy and freedom of expression.

> “Sometimes, the most relevant contradiction that I notice in Tor is that privacy and freedom of expression are opposite to one another. Yet, Tor is providing both of them at the same time. For me this is the biggest contradiction: Tor could be used for ‘revenge porn’ but, at the same time, it provides privacy… it is quite weird”.

4.7. Conclusions: an anonymity and futurity network

The analysis of the data collected during the interviews suggests some useful considerations to close this chapter and to introduce the next one.

a) Although the interviewees referred to privacy by resorting to very different metaphors – privacy as dignity, as a safe space, as the power to make mistakes, as confidentiality of group communications, as trust in infrastructure, as form of personal autonomy, as a privilege or as independence – they all seem to share the idea that this concept has a contextual nature in the sense being defined by Nissenbaum. According to them, privacy is essentially the power to decide whether to share information or not, which information to share, with whom, how and when. Hence, being able to enjoy the right to privacy means to have the ability to selectively reveal data to third parties and to limit the dissemination of such data only to the spheres of everyday life (such as work, family, political activism, leisure time etc) in which one believes that it is appropriate they flow. In this regard, within the Tor community, privacy has been conceptualized either as a mean to limit the circulation of information and, at the same time, to facilitate it.

b) Such interpretation of the concept of privacy reflects in all respects one of the most significant Tor technical properties introduced in chapter 1: namely, its ability to keep together in the same information system different data flows characterized by different levels of secrecy, without producing accidental leaks across them. This is one of the fundamental concepts underpinning the Tor network, whose design, as we have seen, ensures users the power to choose whether or not to reveal their identity to other users and/or to the infrastructure that carries their data. Indeed, the research question that has driven Paul Syverson’s work for 25 year has been precisely "how do you characterize information flow through a system, when you have different levels that are all interconnected?". In my opinion, when he says this, he is basically affirming that Tor aims at creating *plurality* on the Internet, that is to say in an environment whose main feature is *singularity*, as for the first time in history this medium has fueled a widespread perception of the world “as a single social and cultural context” (Tomlinson, 1999). Tor re-enables users to draw demarcation lines between the different contexts of which social life is made, it gives them the power to regulate the access to such contexts and it allows them to put boundaries between public and private again, as well as to create a dimension of separation, unknown and unpredictability around them.

c) In the words of the interviewees, privacy does not exclusively pertain an individual dimension, nor it is limited to the individual as such. In fact, some of informants associate this concept with the ability to conduct a collective action (this is the case of TD1 and KM); others (like TD2) consider it as a tool to re-balance the access and distribution of power and resources; others claim privacy is instrumental to the protection of other values of public interest (such as freedom of expression in Astrid’s case or transparency of the public sphere in hellais’ words); finally, still others see privacy as the necessary precondition for testing established societal boundaries (this is the case of Moritz Bartl). Furthermore, privacy is socially constructed. Indeed, it is affected by specific power relationships (as Alison Macrina explains), by imaginaries that mediate its perception (an aspect emphasized by Nix) or by a conflicting relationship with other high order values (a problem mentioned by Nix and hellais, either in relation to transparency and freedom of expression). Moreover, each of the interviewees stressed the structural character of privacy: in other words, in order to protect a set of values and to constraint the social action that takes place into the Internet infrastructure, privacy must be integrated into the protocols constituting it.

d) Nevertheless, values, ideas and practices which emerge from the interviews and which are made possible by privacy are not bonded by an essence which cuts them transversely, nor makes it possible to read them according to a unique interpretative key. Some of these values refer to an exquisitely liberal ideology, others are more explicitly linked to an antagonistic or anarchist vision of politics, still others (for example, I think about freedom of expression) could be equally shared (albeit for different ideological reasons) by a left liberal, a conservative, an anarchist and a right-wing libertarian. In other words, they do not have an ontological unity but, at the most, they present some features of contiguity, of *adjacency* if we prefer, which are not to be sought on an ideological level (or at least not mainly), but rather in the material configuration of the Tor infrastructure, whose properties and functions, to put it in Papadopoulos' words (2018, 163), "permit only certain development and preclude others".

e) Well, what are these developments? Here the problem is not much that of listing the innumerable Tor's technical properties (traffic analysis resistance, communication security, better encryption, authentication, infrastructure distribution, censorship circumvention, service disruption resilience, geographical position concealment), nor the scenarios in which they can be used. Here the problem is to understand what holds such different visions together, not on the ideological level, but on the *material* one. In my opinion, the answer is that Tor's infrastructure and its design are harbingers of a promise for the

> future. What future? Not a specific future, but *the very possibility that the future continues to exist*. Moritz Bartl and Astrid refer to privacy as the need to have a space for action where one can test new practices and challenge traditional social habits and cultural values. KM and TD1 speak of a sphere of confidentiality which is above all a sphere of collective organization for the transformation of the present. Hellais identifies in the stormy relationship between privacy and transparency a crucial issue to be solved so that the right to be informed is provided by default to citizens and, along with it, the possibility to calling into question the conduct of a political authority. Among the interviewees, Nathan is perhaps the most explicit in relation to the problem of future. Indeed, he emphasizes the importance to make the "ephemeral activities" of everyday life technically possible, so that an individual is not perpetually nailed to her past by the cloud of infosmog that she has produced: in this way she can keep transforming and renewing her identity as she wants, all the times she wants. Also, we should not forget that the relationship between Tor and future was a problem present also in the early reflections of the founding fathers of the network. As we have seen in chapter 1, Mathewson saw into anonymity an important structural condition for favoring free expression and freedom of thought, values that he considered as crucial to encourage a better dialogue between individuals and to solve social problems through a better communication. And when in late 90's Dingledine was working on FH for his master thesis, he had explicitly linked anonymity with the possibility for one to be always able to express uncomfortable and unpopular opinions, in order to prevent any risk of an authoritarian and conservative involution of society.

After all, it should not be surprising that in an infrastructure like Tor, the relationship between future and technology emerges as a matter of primary importance. Actually, surveillance technology is first and foremost a form of mortgage on the future: on the one hand this is because its historical function has always been that of slowing the future down, by crystallizing a status quo and preserving class hierarchies and distinctions (Baumann and Lyon 2013); on the other, because contemporary surveillance implementation is precisely aimed at predicting the future, through a constant construction of the present being operated by big data and algorithms. Yet, if the future can be foreseen, if its development can be traced on a graph, if it becomes a line of continuation of the present, without interruptions, breaks or sudden turns, then it takes on regularity and it is deprived of what makes the future such: that is, the unexpected, the unknown, the dark. In addition, the very fact that surveillance is perceived as ubiquitous (since it has become a constituent component of the Internet) kills the future, because it makes impossible both to imagine a way out from the gaze of the electronic eye and to build an alternative way of life. Borrowing Mark Fisher's words (2018), we could say that rather than a tool for social control, surveillance is actually a political technology being designed to militarily occupy the whole horizon of what is conceivable.

Hence, the liquidity of surveillance – namely, the continuous leaks across different information flows which circulate in the same system and are classified under different levels of secrecy – not only deletes (as we have seen in chapter 1) the boundaries between public and private, utopia and dystopia, state and market, rulers and governed but also those ones between present and future. A collapse that, according to gus, leader of the Tor Community Team, has already taken place.

> "I think that, as Tor Project, we do not have a shared vision of the future. However, I know that dystopia is not the future because people are already living in dystopia and believe that the future is going to be even worse. I think that Tor can be a way out to organize against that. I am not saying that the future is going to be Tor but if you want to have *a future* [emphasis added], you need to have a technology that protect you".

I want to add a short consideration to this valuable and clear-headed reflection. Not only Tor makes it possible to imagine a future once again, but its design and structure *impose* to simultaneously think many possible futures. Obviously this happens because it is an infrastructure specifically created to protect from the eye of surveillance; though it is even more important that its material indeterminacy and the plurality of the functions it performs have made it a catalyst of very different instances, imaginations and political practices which, not only take mutual advantage from their cohabitation in the infrastructure but, above all, are *forced to live side by side* in order to exist in the world.

Not that a person who participates in the Tor network necessarily shares the value of all the other practices which are hosted within it: she simply accepts the fact that in order to make her practices possible, the infrastructure must necessarily make other practices possible as well: practices being potentially very different to hers and towards which she may have no affinity at all. Another way of thinking it: either you accept that within Tor your practices co-exist alongside with practices that you do not agree with, or you resign yourself to the idea that the existence of both practices will be denied by surveillance praxis. If the White House wants that Tor is an effective tool for dissident groups who are active in Southeast Asia, it must also accept that the protesters of Black Lives Matter can use the infrastructure to organize their demonstrations. If the ACLU or the EFF wish that Tor remains a superb infrastructure to protect freedom of expression, they must also accept the fact that this network hosts and protects the presence of Nazi groups[20] who are the most lethal enemies of freedom of expression. If the US Navy wants to successfully keep using onion services as a communications infrastructure for its operations, it must accept that the army of a hostile state can do the same. It is inevitable that this will be the case because, as we saw in the first chapter, the effectiveness of the network is closely linked to the extension and diversity of its user base. In short, *if the condition of existence of surveillance is the collapse of the opposites and the cancellation of the future, then that of Tor is the diversity and coexistence of many possible futures*. As Professor Christopher Kelty wisely suggested me after kindly reading my thesis, Tor is a "futurity" network, being built to safeguard the possibility of multiple possible worlds. Indeed, it can only exist as long as its users are committed to the idea that it might be used for any purpose, now and into the future. This focus on preserving a plurality of possible worlds is the socially and philosophically distinctive aspect of this infrastructure, whose design and organizational practices have been conceived to escape the universalizing character of the Internet.

The politics adopted by the Tor community to configure the infrastructure so that it can host an anonymity set that is as transversal as possible – such as the efforts to increase the accessibility of PETs, the attempts to create new imaginaries around the concept of privacy, the construction of an economic sustainability or the experiments to secure mainstream technologies – has already partly emerged in the previous pages: a more detailed discussion about them will be the topic of the last chapter of this thesis.

5. Tor politics

5.1 Introduction

As we saw at the end of the previous chapter, the condition of existence of Tor is the cohabitation of diversities within the same environment. Furthermore, as we have seen in chapter 1, diversity affects the efficiency of the network as well: indeed, its strength results from the fact that it is used by a set of subjects as wide and heterogeneous as possible. The aim of this chapter is to explore a set of politics (be them technological, cultural and organizational) adopted by the Tor community to configure the infrastructure so that it can host an anonymity set that is as transversal as possible. I refer to the term "politics" as it was defined by Winner (1986, 22), that is "arrangements of power and authority in human associations as well as the activities that take place within those arrangements". More specifically I will investigate three major areas of interest for the maintenance and development of the Tor network. The first one is usability: in sections 1-4 I analyze how this concept is understood as a mean for building the infrastructure in an ethical manner and making the Tor environment more inclusive towards non-privileged people. The second one is sustainability: in sections 5-11 I examine how the creation of alternative forms of sustainability is an answer being elaborated by the Tor community in order to counterbalance the white male and western privilege that characterizes the FLOSS culture and organizational model. The third one is imaginary: in sections 12-17 I explain how the Tor network needs to catalyze a plurality of different imaginaries in order to achieve the technical and political tasks it was created for.

5.2. Security through usability

"The only way to build products that work for the people you want to reach is meeting them, is talking with them"

Antonela Debiasi

Since day zero, usability has been one of the criteria driving the Tor development. The original design document published in 2004 is very clear on this matter: usability is not only convenience, but security as well. The better is the usability of Tor, the higher is the (potential) number of users connecting to its network, the higher is the amount of data routed through it, the lower are the chances for an observer to understand who is talking to whom by resorting to T/A. The importance of usability for the whole platform is mirrored by the same Tor Project's structure. As I write, the infrastructure is developed and maintained by seven teams, each being involved in a different task. Besides the Network team[1], the Metrics team[2], the Application team[3], the Community team[4], the Anti-censorship team[5], and the Fundraising team[6], the UX (User Experience) team exists as well. The mission pursued by this latter nicely sums up the holistic infrastructure management approach being adopted by the Tor Project: "We are making Tor usable for everyone. We act as a bridge between the Network and Applications teams and our users"[7]. Besides the UX team, there are other groups focusing on user experience in the Tor ecosystem. For instance, several members of the Tails development team look after the OS usability.

But what do the Tor developers mean for usability? How does this concept is built into Tor? Which are the elements molding it? And how does usability influence (and in turn is influenced by) other crucial criteria mentioned in the Tor design document and emerged in the previous chapters (such as sustainability or public perception)? In my engagement with the field and the hackers contributing to the Tor development, all these questions came up more than once. I have been helped to figure out an answer to them by two people: Antonela Debiasi, current leader of the Tor Project UX team, and the Tails developer TD1. Let's start with this latter.

From a financial point of view Tails carries on through many constraints and it does not enjoy yet a full economic autonomy. For this reason, TD1 had to take on various tasks related to the management of the Tails infrastructure. Among them, there is the accountancy of the organization, the management of its website and, in fact, the improvement of the UX. He does not have a specific training in this field and only recently he has started to deal with it. I find interesting, and somewhat revealing, the way he conceives usability. In his perspective, this word stands for "attention" or "sensitivity" towards users.

> "For me usability is making sure that a tool is relevant and understanding why it is relevant and for whom it is relevant. Usability means either making sure that the people you want to help can actually use such tool and doing what is required to be done in order to make it useful".

According to TD1, in order to make Tails usable and relevant it is pivotal to understand

> "how the tools that we build really work for people, if they are useful for them, if the users can achieve what they want to do with such tools, if it is easy, if it is complicated. From that observation we try to make the tools we designed more useful and more easy to use".

Talking about usability, Antonela Debiasi uses similar words: "Usability is about making sure that anyone, no matter her technical background, can use a tool". Easier said than done, because, as she explains me, usability is a difficult condition to embed into any software in general, and even more difficult in Tor-based one in particular. The reasons are various and range from the specific goals Tor was designed for, to the context many users live within, to some cultural trends crossing the community and characterizing its identity.

5.3. Acting as a bridge

Antonela starts to tell her experience as UX designer by problematizing this latter aspect. As we have seen in the previous chapters, Tor is an organization with a strong academic background, largely made up by people that she defines as "solution thinkers moving in a controlled environment". There is no anti-intellectualist stance in her remark, nor she distances herself from the work of engineers such as Syverson, Dingledine and Mathewson (to name just a few). Antonela just observes that there is a gap between a lab prototype built by a scientist and the use that Jane Doe could make of it; a gap that, if it is not filled, could make every technology, even the most sophisticated one, useless in real life. "As we write on our home page, the UX team acts as a bridge. Our work is connecting the academics with the rest of the world [...] We try to match the reality and our real users with academical findings". However, her task is not simply matching academic findings with reality. Her aim is actually designing and building open tools involving academia instead of taking isolated path.

> "We are solving complex problems. We need diversity in our decision-makers in order to reach the most plural user base. This is the 'bridge' part of our work".

To explain me even better what 'to act as a bridge' means, she tells me about an episode she experienced in 2018 together with Alison Macrina, former leader of the Tor Community Team.

> "Last year, me and Alison went to Uganda to run this security workshop and a usability test. We went to the capital and then to this city called Oima. The city is changing. A company found oil in the soil: they are exploiting the natural resources of this area, a lot of money is flowing. So, we meet this group of people who were environmental activists. They were all men. Some of them were journalists, others were bloggers, others were people working for local newspapers. We started the workshop. Everybody had his own old computer and everybody was using Windows 95. The internet infrastructure was pretty weak: we got less than 2 MB/S for downloading and the data package was really expensive. Finally, we managed to start the workshop. However, after five minutes the power grid went off. Puff. A blackout! Alison and I were like: "OK, we do not have computers, let's think about something different to do".

Despite the obstacles, the trip to Uganda was a success. Or perhaps, it would be better to say that it is precisely because of these obstacles that it can be considered as such. Antonela's tale perfectly sums up how user experience is affected by a series of crucial conditions which cannot be ignored nor taken for granted by any mean. Among those, the technical background of the user (usually non-existent in terms of security, privacy and online anonymity), the hardware and the software available to her (often limited, or even obsolete one) and the infrastructures being used (a reliable power grid and/or cheap mobile traffic are a common condition in Europe and in the United States, but this is not necessarily true at other latitudes). It is impossible to positively address each of these complications – there is obviously little to do in case of a local power plant blackout – but some of them can be dealt with.

Yet, Antonela says, it is difficult to explain this kind of scenarios “to a developer who lives in North Europe. He has never had a power outage” and through his life “has always had a good internet, even at a night time”. And it is equally difficult that an engineer could envisage this kind of issues while she is developing a prototype within the aseptic walls of a research lab or in the halls of a university campus. When one works on a technology still being in an experimental stage, usually the only concern is that of making it fully operational. You don’t lose too much time thinking about a potential user base and therefore bending its functionality and features to specific needs rather than others. As another hacker, who asked to remain anonymous, explained me “in this particular phase of development, the end-user is me. If the software is not even good for me, how could it work for someone else?”. Moreover, in the case of Tor there is another problem that makes it even more difficult to fill the gap between end users and developers. As we have seen in the first chapter, among the different goals Tor was designed for there was also that of protecting the civil rights of European and US citizens. In other words, onion routing was originally created with liberal political regimes and technologically advanced infrastructures in mind. This feature does not make simple nor immediate its re-conversion for other contexts.

Nevertheless, a failure to acknowledge these matters represents a limit either for the network effectiveness and its extension range. As Antonela tells:

> “if we do not think solutions for this kind of contexts, we are leaving people outside […] if we do not care about these situations we are making a boundary, a border of exclusion of the people we are reaching”.

And she adds:

> “Tor has been developed by northern white males. I want to emphasize that being part and pushing code onto an open source project means to enjoy a privileged condition. Most of the time the people who do not have the technical background to fix a given problem, who do not have the technical background to understand this tool, is the people who most need that. And

> they are left out. If we do not take that into consideration we would be… well the word in Spanish is “egoista” (selfish)”.

Therefore paying attention to the users, their needs and their problems is a listening exercise aimed to make the Tor network more inclusive: no one must be left behind, nay, no one must be left out. Everybody has to be able to resort to an anonymous channel of communication. But how such inclusiveness could be built? For whom? For which social groups? And where?

5.4. Building usability in an ethical manner

Antonela has been working for a long time as a digital product designer in several for-profit industries. Metaphorically speaking, we could say she had been on the other side of the screen and she well knows how Internet companies build usability of their products. In most cases, they resort to telemetry, that is, very powerful spy software[8] being designed to record every slightest movement of the mouse cursor on the screen. It is rare for the user to be aware of their existence. Telemetry technologies are just invisible. Sometimes they are concealed within software source code. Some other times they could be found within the ToS that we subscribe hastily and out of boredom before starting to use an app, thus granting its manufacturer the right to constantly monitor us. Data collected through telemetry are sent to the parent company, stored and later analyzed as an aggregate, in order to study the behavior of millions of users and understand how a software GUI (graphical user interface) can be modified and be made more accessible.

Well, this working method – that, Antonela tells me, it is basically the ICT industry standard – cannot be used by the Tor developers. Never. Under no circumstances. And not because its use would not be useful or convenient for them. Simply because they cannot afford to adopt it and integrate it into the Tor Browser development cycle. As Antonela tells:

> “We have this long-term collaboration with a browser vendor, we collaborate often with. They have telemetry, a tool which measures their

> users' behavior. It works very well. Some time ago, I went to this meeting and one of their developers asked me: "I would like to know how many times Tor Browser users open the onion circuit display". "Well, I do not know" was my answer. He looked at me, quite surprised, and said "You should run telemetry on that! You should know how many times people are opening the circuit display!". Obviously, as I explained him, it is not something we can do. We cannot fail with this. There are people who use Tor Browser and are in real risk. It is not that I am a paranoid person. The thing is that Tor Browser users – people who I have meet, known, who have real names, faces and stories – often live under governments who arrest them, kill them, seize their computers. The local police is going to knock down their doors, take their hardware, open it, possibly know everything about their family, their work contacts, their habits. For sure they will use it against their activism. And sometimes, the activist work is not even something radical, it is just people who want to check Facebook".

Resorting to telemetry in order to enhance Tor products usability is just out of discussion. The users' security could be compromised. A single error in its implementation could put in jeopardy the safety of an unspecified number of people. And even if the implementation of such technology within Tor Browser would happen without errors, the Tor Project would still have to take on the responsibility for stocking the data being collected, thus further increasing the infrastructure management costs and making it a potential target for anyone determined to seize such data. Moreover, the blatant contradiction of a network that claims to be privacy-preserving and, at the same time, integrates in its development process techniques specifically being designed to violate privacy would immediately catch everybody eye. Such a choice would be hard sell to millions of users: it would make difficult to keep their trust and preserve a positive feeling about Tor, with the consequent risks for the dimension and the diversity of the anonymity set (and therefore the ability of the network to effectively comply with the task it has been designed for). In other words, resorting to telemetry techniques in order to enhance the UX would imply a series of consequences and technical, ethical and aesthetic implications which could be potentially devastating. Consequences that perhaps an engineer working for an important browser company (and who hardly faces similar scenarios during his daily routine) could not think of, but which instead are basic assumptions for those, like Antonela, who are accustomed to work closely with users at risk.

There is coherence between the method she uses for developing the Tor Browser UI (user interface) and the values it should embody and promote. In order for a software not to be selfish and to be free from barriers preventing a wide user base to employ it, it is necessary to write its code in an empathetic way. Antonela creates security through empathy. It is worth to briefly ponder the meaning of this term because, by reflecting on it, we can understand the huge distance that, at least in this case, separates the Tor ecosystem from the one of the mainstream ICT products. Being coined by Robert Vischer (Vischer et al 1993) at the end of the 19th century, empathy is a term referring to the individual ability to 'feel inside', to perceive the feelings and the state of mind of those surrounding us, and of nature itself as well. When we are empathetic, we feel together with someone else what she is feeling. Empathy requests consent (a word that, in Italian, derives from the verb 'consentire', precisely, to feel together), common agreement and reciprocity. Exactly the opposite of what happens when a developer uses telemetry, a technology akin to an invisible implant under the users' skin, being brutally inserted in order to quench the Silicon Valley unbridled desire of personal data. A greed, a covetousness, a selfishness indeed, that is mirrored by the use being made of these data: first, they are embezzled (through force or deception) and later they are interpreted and elaborated according to an exclusive perspective (the one of the developer) that gets translated and imprinted into the code.

On the contrary, Antonela's approach to UX postulates and reflects an explicit idea of mutual collaboration between users and developers. Her vision drawn upon the concept of open and collaborative design methodologies conceived by Sundblad (2011) and it is affected by the notion of human-centered design[9]. Moreover, being Antonela a cyber-feminist, she aims to build technological infrastructures characterized by decision-making processes being strongly grounded on mutual consent[10]. As Isabella Bagueros, former UX team leader and now Tor executive director, wrote in an e-mail she sent to the Tor's UX mailing list "we do not know what is good for the user" [...] "we must test what we build with them to actually know if we are doing right". And she added: "We are building a way to do user testing with the help of trainers and users all around the world, by creating a direct interaction with them instead of collecting behavioral data about them"[11].

With them and not *about* them. It is the choice of a preposition instead of another that gives meaning to a discourse and to the practices resulting from it. It is all about consent. It is not by any chance that, as we have previously seen, the concept of privacy is often associated by the Tor community members with the idea of expressing consent about which personal data can be shared and with whom.

5.5. Putting a face on people for making them anonymous

In order to feel what users feel, Antonela travels continuously. Every month she takes a plane and goes to Central Africa, South America, Middle East, South-east Asia. Like a wobbly, she is present everywhere people are fighting a liberation struggle and are using Tor to carry it on. Not that she is rich and travels around the world like a philanthropist. Her journeys are part of a three years program being funded by a European development cooperation agency with the aim of expanding the use of Tor in the Global South[12]. Until this moment several members of the Tor community traveled to India, Indonesia, Uganda, Kenya, Colombia, Mexico and Brazil, training people in digital security and also collecting feedback about the usage of apps and software[13]. The workshops and the usability tests she runs together with these activists are fundamental.

> "If we do not feel the same experience, the same fears, the same expectations that users feel, we cannot involve the human perspective in the problem solving process".

Surely, this methodology implies relevant economical expenses (obviously being entirely paid by the Tor Project) and limits. The amount of data being gathered is far from being massive and it is collected on a smaller scale than what it would be possible to do with telemetry. Moreover, data processing takes longer than usual because it is run by humans and not machines. Nevertheless, the benefits of this approach are not negligible. Firstly, because the privacy of those voluntarily participating to these tests is not compromised by any mean. Secondly, and most importantly, because such tests take place through personal interaction. The user is not a statistics any more, nor a set of numbers being allocated in the table of some obscure database situated in a SoCal-based company intranet. On the contrary, she takes – a rather curious fact for an anonymous network – a face, physical features, a context she belongs to and she acts within. She becomes a real story that Antonela brings home and tells in the IRC chat where most of the Tor life takes place, or during the half-yearly meetings organized by the Tor community.

> “Thinking about real user cases, thinking about real scenarios, thinking about personas is what we have been doing and I think it is the main improvement provided by the UX team. We have done exactly what we should have been doing long time ago: putting voices on these user cases which are extreme, which are exactly the people we want to reach, like activists or people in real risk. I need to share real histories that the developers can understand, the real needs of people, and this is something that is part of my team, the story I want to bring to the discussion. I mean, without this kind of discussion we are making many decisions which are irrelevant to the users. I make my suggestions from what I find from users directly, put the users voices on the development process. It is a kind of ‘I have been with these users, this is happening to them right now, these things happen for real: can we try a solution for that or are we going to keep this outside?’”.

These real stories are the bricks that Antonela employs for building the bridge connecting the Tor developers with the real world[14]. They perform the peculiar role of the mediator, that is, connecting what is separated (Zielinsky 2006). Making the users anthropomorphic beings (and not just numbers or statistics) is a mean to fill that gap that could isolate an engineer in his comfort zone, thus making Tor hardly effective, if not even useless. If usability, as the Tor design paper suggests, is a security parameter, then also the ability to develop empathy towards other cultures should be considered as such. Paradoxically, even the most selfish Tor user could want to develop such empathy (or at the very least to see it embedded within Tor) for pure self-interest. Widening the diversity of the points of view embedded within Tor, going beyond the cypherpunk perspective, that of the military, that of the academy, that of the political activists in the global north means making the network more usable and therefore potentially more crowded and strong. It is a problem that Antonela summarizes as follow:

> "Often the best solution that we found to improve the Tor Browser was to delete some of its components from the UI. Do you know why? Because users did not know how to deal with them! I mean… We just cannot tell them 'Hey guys read the fucking manual [RTFM] and become a network engineer before using the Tor Browser in order to circumvent on-line censorship'".

It is a perspective that matches what TD2, another Tails developer, tells me:

> "I come from training activists. We tried to raise awareness and teach them how to build their own security policy in order to decide how much they want to invest on this and which kind of tools are most suitable for their needs. At some points we noticed that we were trying to change the people, to adapt them to the tools and we thought: 'OK. We do this with some people today. Then the next day. Then the week after. Then they forget what we taught. But we are not so many and there are 6 billion people to educate! This approach, this strategy is not working. We need to change the tool so that they behave safely, better and so people just need to know how to use them and not how to work around the tools'. This is how Tails started".

Those described by TD2 and put in practice by the Tails community is a huge shift in hacker culture. It is not only an attempt to listen closer to the vast world existing outside the hacker conventions held in Europe or in Las Vegas, but also a way for putting into questions some of the fundamental FLOSS cultural assumptions in order to re-negotiate them with millions of users now excluded from the infrastructure. "RFTM![15]" is not an answer that could be given to somebody in trouble and who is experiencing difficulties in using Tor Browser. Similarly, the idea that just spreading awareness about good tools to use and best practices to adopt was a winning strategy in order to protect people privacy, eventually proved to be an illusion: indeed, its feasibility was reconsidered because it proved to be unenforceable outside small worlds being paved with white male privilege and inhabited only by little swarms of hackers, FLOSS enthusiasts or activists.

The Tor development occurred in the last two years shows that in this perspective things are slowly changing for the better. In May 2019, after several months of development, the first Tor Browser version for Android officially supported by the Tor Project was released: this app was explicitly designed for those areas of the world where the Internet is made accessible only via mobile connections and low-cost phones[16]. Moreover, in the same period the Tor protocol was improved in order to decrease power consumption, and thus make onion routing less battery demanding when run on a smartphone[17]. Lastly, Antonela tells me that the next step of Tor Browser will be that of becoming smarter and, if required, making a decision for a user if she thinks to be in a situation at risk and does not know how to deal with it.

5.6. Security through sustainability

> "Contributing to an open source project is a luxury. Only privileged persons can afford it".
> Hellais

During the interviews that I conducted, it has often emerged how the open source organizational model upon which Tor is based presents several flaws – particularly in regards to its sustainability – that the community has been trying to dealt with by adopting different strategies. Indeed, along with the cultural values and virtuous principles characterizing FLOSS, Tor has also inherited many issues resulting from the scarcity of resources affecting this environment. As claimed by Eghbal (2016a), one of the consequences of such scarcity is a reduced diversity of the subjects inhabiting the FLOSS ecosystem: particularly, low incomes and the lack of a long-term employment perspective make it hardly accessible for those not already being provided with their own economic resources, thus creating a "selection at the entrance" that reduces gender, class and ethnic diversity within it. Formenti (2008, 254) explained how this dynamic determines a hierarchy within many FLOSS communities because "a relatively small number of developers participate in the most important projects, while the mass of amateurs is dispersed in a galaxy of peripheral activities that marginally affect the evolution of top products". Nafus (2011) argues that FLOSS is fare more male dominated than other forms of software production and its daily practices exacerbate the exclusion of women. Given that Tor's condition of existence is the cohabitation of diversities and network efficiency depends on the transversality of the subjects who use and maintain it, how is the infrastructure affected by the 'selection at the entrance' dynamic characterizing FLOSS practices?

"Contributing to an open source project is a luxury. Only privileged persons can afford it". This is Arturo Filastò's opinion, leader of OONI, as well as founder and developer of the whistle-blowing platform Globaleaks. Arturo has been a member of the Tor community for a while now and he is well aware of this issue. In his own view, as time went by Tor has become more inclusive from a gender perspective. Yet, he is also very clear in saying that the lack of sustainability of the project and the scarce diversity within it are problems that, although toned down, persist in structural terms. And, like for any other open source project, the solution does not seem to be in sight yet:

> "…being a voluntary to a software project, making a contribution in all the debates happening on the mailing lists and taking part to the code-writing process or to the infrastructure administration is a great privilege. Basically, it is not something that everyone can afford. This necessarily leads to 'a selection at the entrance'. I do not know how we can address this problem".

A problem that Alison Macrina, former leader of the Tor Community Team and director of LFP, explicitly links to the lack of salary provision. Free labor is definitely not a vector of diversity:

> "We have to look at the whole picture. If you demand your project to depend on free labor you have to think about who is in the position to give their labor away for free. Certainly it is not women, it is not people with family, it is not people who have multiple jobs".

According to Alison, the gender issue within Tor is a complex problem being rooted in the FLOSS breeding ground. The first time we meet online is August 2017. Little more than one year earlier the whole Tor community was shaken by the so-called “Jakegate”, a sex scandal which featured Jacob Appelbaum as its protagonist[18]. Famous on the web with the nickname *ioerror*, Appelbaum had been for several years the most prominent Tor Project spokesperson: a role granting him a social credit and popularity that only a few could boast in the European and US hacker scene. In May 2016 Appelbaum is publicly banned from the Tor Project, following a number of rape and sexual abuse allegations that his victims decide to bring out. Alison is one of them and partakes (initially by using an anonymous identity) to the creation of a website[19] where evidences against Appelbaum are collected and made public. Few weeks after the outbreak of the scandal, Macrina publicly takes the stage first-hand and writes a post on Medium[20] in order to comment the issue. Surprisingly, the polemical target of her writing is not Jacob Appelbum, or at least not just him. Alison elaborates an articulate analysis where, rather than lingering on Appelbaum’s predatory behavior, she focuses instead on the cultural elements present in the Tor community that have made it possible. Among these, a ‘star culture’ that allowed a single individual to concentrate into his hands a significant share of power; a ‘shut up and code’ mentality that made a positive human interaction among those participating to the project increasingly complex; lastly, the rise of a ‘bandwagoning process’, a concept that could be summarized as follow: in order to ride Appelbaum’s coattails and to enjoy the fame and the opportunities resulting from it, it was enough never to contradict him. Not even when somebody was accusing him of rape.

Centralization of power? Frantic quest for visibility? Establishment of an absolute and unquestionable authority? How was it possible for such dynamics to insinuate into a community whose ethics is based on principles like “mistrust authority. Promote decentralization” or “hackers should be judged by their hacking, not criteria such as degrees, age, race, sex, or position” (Levy 1994)? How was it possible that, in front of the emergence of political and personal controversies, a group of people who dedicated their whole life to the creation of a censorship-resistant infrastructure had choose silence and uniformity of thought, instead of trying to settle such issues with a frank and open discussion? Alison has several answers to these questions.

> “How did abusive men get in the Tor world? We are still examining the way we have been participating in that as an organization. However, the cultural elements that made this possible became part of the community because, unfortunately, they are really fundamental to FLOSS. When we think about the history of this movement we should not forget it is fundamentally structured around men, all of them being white, from the global north and from that part of the global north that is rich. These men have done extraordinary things, they have very powerful words, they have built technology that I use every single day. One thing that all of these men have in common is that they are all pretty abusive. Linus Torvalds is an example. Eric Raymond has said very racist things. Julian Assange is another example. And many more. However, it is such a paradox because in a culture that values decentralization, rational thinking, skepticism and all these things no one has been willing to criticize any of their heroes. I do not know what the correlation is between FLOSS and sexism. Maybe there is no correlation, but what I do know is that Tor was not immune from it in any way. […] It is so ironic that basically free software is one of the most principled endeavors that I have ever seen. It is really ‘we believe in these principles, no matter what’. But then any other principles that come up do not matter”.

There is another interesting aspect to emphasize about Alison’s words. That is to say that the presence of these power dynamics within Tor have been reason of (self)exclusion, not merely for people who became the target of abuses but also for those ones who, even if not being first-hand affected by these behaviors, found them to be reprehensible and therefore decided to take a distance from the community, or not to get in touch with it.

> “I joined Tor in 2014, like at the end of 2014 and then I got really involved in 2015. And then it was at the end of 2015 that Jake assaulted me. I think that, just like other FLOSS projects, there are other elements which are important

> for allowing this to happen. Not only people thought that men like Jake were so cool and did not want to criticize him. These men take advantage of the fact that, even if Tor is a mostly male dominated environment, they are not all the same kind of men. Lots of these men are rather timid, some of them reflect the kind of cultural stereotype of the socially isolated hacker and they get abused by the "rock stars", too. Because these men, they are not willing to stand up to them, because they resemble the guys that bully them in the high school, too. So, in a lot of ways, this is like a perfect environment for an abusive person to thrive in because there is no one else to stand up to them, and anyone else who will occupy that kind of power will look like them. What I understand of the history is that there are many who objected to his behavior who just quietly left. And I think that this is something that has happened for years".

Beware: the boundaries that define the Tor community do not stop here. There are other forms of exclusion, that go beyond the "jakegate" and that are due to what Alison (but also other members of her community like, for example, Antonela) defines as a "global north dominance issue".

> "We have really been trying to participate in communities in the global south and not like 'We are the creators and they are the consumers' but like recognizing how we have failed to integrate people form the South in our community. And we have invited a bunch of people from the whole global south in our last meeting. We had this session where they basically told how angry they were at us. This happened because we were supposed to be this principled organization. The reality is that we have been replicating the same power structures they have seen from the US worldwide. Let me make an example! We have those meetings two times per year which take place in different parts of the world every time. And when contributors from the South said 'Would you consider having a meeting in a country that is not in Europe or North America?', for years we made all kind of excuses: the difficulties of getting a visa, the cost of the travel the lacking of a proper

> infrastructure…but the thing is that all of our contributors make more money than folks in the south. It is actually easier for them to get visa from the south rather than the opposite. We have not even considered the power structures entailed into this way of thinking. Is it difficult for all the people in Sweden or whatever to get to Chile? Well, this is what the reality has been for contributors in the Global South for the entire history of free software. We can inconvenience ourselves a couple of times".

As it happens for many other open source projects, Tor is (or in the past was) crossed by gender and class power relations which produce forms of abuse and exclusion. Yet, Tor is not an ordinary FLOSS project. Indeed, as per the title of an old paper authored by Dingledine and Mathewson (that later became a frequently quoted leitmotiv by the community members), anonymity loves company. According to the authors of the study "while security software is the product of developers, the security it provides is *a collaboration* [emphasis added] between developers and users. It's not enough to make software that can be used securely – software that is hard to use often suffers in its security as a result" (Dingledine and Mathewson 2006, 1). This is because, as previously explained, better usability means a higher number of users, and a higher number of users means higher security. Security that, as Dingledine, Mathewson and Syverson claim, increases with the growth of the anonymity set diversity. Indeed, "if Alice is the only user who has ever downloaded the software, it might be socially accepted, but she's not getting much anonymity. Add a thousand activists, and she's anonymous, but everyone thinks she's an activist too. Add a thousand diverse citizens (cancer survivors, privacy enthusiasts, and so on) and now she's harder to profile" (Dingledine et al 2005, 5).

But how can a uniform community endorse the creation and the maintenance of a diverse infrastructure? In other words, how can a community – one being perceived as non-safe for women, crossed by tendencies of authority centralization, organized around a few indisputable cultural principles, devoid of sources of income and only accessible to affluent, white, male programmers hailing from United States or Europe – reproduce and incorporate such diversity in the digital artifacts it builds? In the next sections I will analyze the role of the existing Tor's funding system in relation to the above mentioned issues in order to understand whether or not it has been useful to mitigate the flaws affecting the FLOSS organizational practices. In parallel, I will analyze the efforts made by the community to create a more inclusive, not-western, not-male and not-white centered organizational structure.

5.7. Chains of funding

As we have already seen in chapter 3, grants provided by the NSF, the DoD and the DoS have surely produced a positive outcome on the Tor's organizational arrangement. Although they are not huge sums of money – just about 16 million dollars in a period ranging from 2007 to 2016 –, they made it possible to hire full-time engineers, programmers, designers and other professionals who hardly could have contributed to the infrastructure development without receiving a salary. Nevertheless, such funds were not enough in order to create a long-term economic sustainability for Tor. Moreover their origins, their modes of delivery and the purposes they have been made available for triggered the rise of new organizational and technical problems within Tor. Let us see why.

First, how does the Tor funding system work? In chapter 3, I partially answered this question by explaining which are the goals that lead several US government agencies to fund the infrastructure development. Now, I would like to reverse the perspective and deal with this problem from the Tor Project's point of view by using documents, interviews and other information that I collected during the fieldwork. Among the materials I have taken into account there are footage of some public events attended by several Tor core people during which this issue has been publicly discussed. One of these is the Chaos Computer Club Congress which takes place in Germany, usually between Christmas and New Year's Eve. Until a few years ago, on this occasion the Tor Project used to hold a panel named "State of the Onion" in which two or more spokespersons (Roger Dingledine was normally one of them) informed the audience about the progresses made by Tor during the year. The topics discussed were various: some of them could be technical (like the new features introduced in the stable release of the software, or the new projects based upon the Tor network); some others could be related to the organizational dimension of the project (for instance, the election of a new member in the board of directors); some others again could be more political and cultural (i.e. the importance to create a positive perception around the concept of online anonymity). During 2013 State of the Onion[21] Dingledine explained some of the fundamental principles of Tor's funding system as follow:

> "Funders usually have a project they want Tor to work on. We go to a contractor and we tell them: we have ten things we want to work on. If you want to fund one of these ten, you can help us to set a priority [...] if you have funding for one of these we will focus on the one that you are most interested in".

These words show how the priorities of the Tor development are neither entirely set by Tor Project, nor by its funders: rather, they are the result of an agreement between them. As pointed out in the blog post that made 2017 financial statement public[22], funds received by Tor Project are not the result of a top to down process and, the article emphasizes, "there is never any point where somebody comes to us and says 'I'll pay you $X to do Y'". On the contrary, first Tor defines a set of projects that its developers are interested to work on. Then, in a second moment, it submits a certain numbers of applications to different funders who, in turn, make a selection and pay a grant for the ones they are interested in. The disburse of money occurs according to two typical contract models, usually employed by non-profit organizations working with governments or public institutions. The first one is called "cost reimbursement" or "fixed-cost". With cost reimbursement, an organization who benefits from a grant has to justify the way it has spent the money in order to get paid. In other words, it has to demonstrate that the goals it achieved are actually compliant with those ones previously agreed with the funder. The second contract model is the "milestone-based" one. With this latter, an organization envisages a project as if it was a list of sub-goals, then defines a roadmap to achieve each of them and finally brings it to the funder's table. If the funder agrees with the plan, then for each milestone being achieved by the grantee, a previously established amount of money is paid. As explained in the above mentioned post, "the milestone based model give us more flexibility to do all the things that need to get done (e.g. we can choose prices that accurately reflect the maintenance costs too), but it can also be more risky because it's on us if we underestimate costs".

The people that I interviewed described the "milestone-based" contract model and the "fixed-cost" one with very similar words. Yet, they have added interesting details which proved to be very useful in order to better understand the relational nature of the Tor infrastructure. As Arturo Filastò, OONI leader, claims:

> "We get several funds from the US government but, contrarily to what people think, it is not like they come to us and say 'Hey Tor! Develop this feature so that we can crush the Chinese'. Basically, we have things in mind, we need money to do those things, we look to the donors we are already in contact with, and explain them what we want to do. Usually they reply us: in order to get money from us, instead of phrasing this thing like that you should phrase it in this other way – so the proposal has more chances to be accepted".

Hellais (that is Arturo's nickname) explains more in detail this last bit.

> "Funders are always akin to a series of chains. We receive money from a US government body (let's call it "agency X"). This body receives money from another "institution Y" within the US government. In turn, "institution Y" receives money being allocated by US senators who receive money from US taxpayers. Why am I saying this? Because, as we have to justify how we spend the money that an institution give us, such institution has to do the same with another institution as well. At the end of the day, in most cases what matters is not much what you do (that in 99% of cases is what we want to do, what we would do anyway). Everything is about how it is phrased and justified to the funder, who in turn justifies it to its funder and so on. Basically, funding works like this: we have in mind what we want to do – that results from what Tor users tell us – and we plan our objectives as an independent NGO. And then, on the basis of what we want to do, we find the right institution interested in funding our work".

Also TD2, one the Tails developers I have interviewed, is even more explicit in regard to the meaning of the verb “to phrase”

> “If you write your grant proposal for a US cooperation agency, you are not going to talk about Snowden, Greenwald or Laura Poitras, at all. You explicitly should not. You should talk about China, Belarus or Syria. That is what they want to hear. That is the kind of proposal that they could accept within the boundaries which are in turn established by the US Congress”.

while TD1, another Tails developer, similarly states that:

> “The funding comes with very little conditionality, of course you have to apply and you have to give them goals, and you have to make these goals aligned with their goals, and then they say ‘go for it!’. But, when we applies to such funds, we always apply with our own priorities, and then they never tell you to do something else with the money. We have our own priorities, and we share priorities, and they give us the money and both are happy”.

This ‘alignment of priorities’ is a kind of undeclared agreement between the parties involved. As Nix, an anonymous researcher whose work has been previously funded by a governmental organization, explains me

> “There is lot of awareness and complicity with the guys of these funding agencies. On the one hand you can honestly state how your technology can be useful to the their agenda (and therefore to the DoS agenda). On the other hand, it is also clear (even if it is not explicitly said) that this kind of technologies will be used in countries where there is a lot of civic awareness, rights and were there is a good digital infrastructure with lot of connected users. [...]. It is obvious that in order to get funds we created a frame according to which ‘the dissidents can speak anonymously with the journalist without being wiretapped by the bad government’. This is the story that must be said by the DoS. The reality is that the majority of our users, and the majority of the platforms based on Tor, are in western countries. If funding agencies and the DoS want to sell each other the frame

> of the dissident fighting an oppressive government with Tor… it is their problem. What it happens is a different reality”.

Senators, politicians, NGOs, ministerial boards, funders, activists and hackers. Everyone bound to the other like in a chain. Everyone winking at the other in order to guarantee herself the highest advantage (both in political and economical terms) at the minimum cost, everyone staging a role, playing a part, preserving their public image and sticking to their priorities.

5.8. Building infrastructures with masking tape and wire

By reading OTF reports, one can easily comprehend how a whole ecosystem of privacy-oriented technologies has benefited from this funding chain for years. Without the money that Washington has disbursed, Tor would probably still be what it was in early 2000’s: namely, an experimental protocol only running on a virtual machine in an obscure governmental research center or (as it happened with Free Haven) a genial idea for a master thesis that, as soon as it was implemented in real life, showed flaws that made it useless.

Nonetheless, it is true that over time the source of these funds (that is a few US government agencies) has created and continues to create problems to the Tor’s reputation, both inside and outside the community. Actually, outside Europe and US, the perceived closeness between Tor and Washington seems to be a hurdle in terms of inclusiveness and capacity to expand the network. Indeed, according to Alison, this funding system “has so many failures modes, particularly for what concerns the distress that it generates for people coming from the Global South, people who have really bad experiences with the US imperialism”. And, as above mentioned, this is a problem being diffusely perceived within Tor as well. When in 2015 Shari Steele took office as new executive director, one of her first acts was doing an internal survey in order to identify the issues experienced by the employees of the organization[23]. Notably, 30% of them expressed discomfort about the current funding system, as they see it as an element undermining the Tor’s credibility: a good reason, they said, to stop to take money from the US government. The Tor Metrics figures seem to confirm the soundness of this concern. As a matter of fact, if we look to Latin America (a continent counting 415 million people) we can see how there are only 132 running relays, 82 of them being in a single country, Brazil (as I write, the running relays are 6568).

Nevertheless, there are more reasons because these grants are not only a resource, but also a limit to the development of the Tor infrastructure. The first one is their purpose. These funds are meant for research and their delivery, as we have earlier seen, is mainly bounded to the achievement of quite definite milestones. It is absolutely natural that Tor people chose to resort to such a mechanism in order to support the network development. Indeed, as stated by Shari Steele in an interview, the engineers and hackers who originally created Tor "have built the organization around a university research model where they fund specific projects and have to have separate budgets for each of the projects they're working on"[24]. As Alison adds, such approach "reflects the origins of Tor, because the original people who worked on it were researchers and the only way they knew to get money was research grants. That's why lot of Tor money is research grants".

And this is a huge problem. Indeed, Tor is not only about research. Tor is infrastructure, therefore it is administration, communication, coordination of activities, resolution of bureaucratic and accountancy problems. Adopting an organizational model meant for advancing university research in order to manage a communication network is a wrong choice. In an interview released to the press, Shari Steele described this problem with a metaphor which brilliantly depicts Tor's lacking of flexibility, an organizational problem which can be easily overcome when one is running an academic experiment but not when one is managing an NGO or a company.

> "The Tor team has resorted to using 'masking tape and wire' to solve their operational challenges. It really is a case [...] of really brilliant people coming up with an answer of how to solve something when they don't really have any knowledge of how it's done in other places".[25]

This lacking of flexibility results in a slower development process. As it has been explained in a Tor blog post[26]

> “the traditional grants that nonprofits normally depend on, be that from governments or private foundations, have a long turn-around period (six to twelve months from submission of a proposal to the receipt of a contract and start of work). That means when a proposal is accepted and a grant contract is signed, we begin work on the project that we outlined sometimes more than a year prior”.

Then why the Tor community made the choice of adopting such funding model? The answer is simple: it did not make this choice at all. On the contrary, this sustainability and infrastructure management model is a legacy coming from Tor early days, when the platform was a playground for geeks and not a communication network employed by millions of users. This is a well know dynamics in infrastructure studies. It reflects the inertial qualities of any infrastructure which “pointing to the fact that, once established, systems tend to continue in particular directions, making reversals or wholesale leaps to alternative approaches costly, difficult, and in some cases impossible” (Jackson et al. 2007). According to KM, one of the Tor core people I interviewed:

> “I guess people are a bit trapped in the funding cycle because they know how it works, what they want and they have already an established network of contacts in order to get it”.

5.9. Nobody pays for maintenance

What is this trap about? The answer to this question is articulate. First of all: many funders, particularly those belonging to the organizations tied to DoS, do not have a clear idea about the complexity underlying a process of technological development, nor actually they seem to be interested in having one. As TD1 explains me there is “a big divide between what these people know about technology and what the reality of technology and software development is”. This gap can imply disagreement among stakeholders in regard to funds allocation.

> “Funders want new apps and software. They want innovating solutions so that we can have lot of impact and prototypes. [...] It is the same for all the

> foundations: when you write grant applications they want only new stuffs, new features, stuffs that have a real impact but it is very hard to get funding for maintenance, sustainability, usability and this kind of more background work, because it is not sexy for them. They always want new stuffs because they want to report to whoever give them money that they did something right, something great and something new”.

And this is a big problem because

> “some of us could be busy full time just by doing nothing, just by making sure that Tails still works with the next version of Tor, with the next version of Mozilla, or by pushing up releases for security fixing and without adding nothing of new to our distro. Only keeping Tails up to date with the security patches of the software we ship, or keeping it working with the new version of Debian, or keeping the infrastructure running, or staying up to date with the new versions of Firefox and all these kind of stuffs… well, only these maintenance tasks would keep at least a couple of us completely busy. We have to keep up to date with the whole ecosystem. In Tails we ship tons of different software, we rely on GNOME, we rely on Debian, and our infrastructure relies on different types of software as well. Everything changes all the time. Just to keep Tails working and not adding everything is already a lot of work. This is just the technical one and you need to add the administrative one. You need to make sure that the organization is running, and you also need help with this. These are not new features of fancy things, but they are required in order to keep the infrastructure working. It is something that we need to do to stay alive. It is lot of work and we need to get paid to do this kind of stuffs”.

Here we have two forms of relationality of the infrastructure that clash with one another. On the one hand, there are funders, who are organized in chains, with each ring of the chain depending on the next one. In order to be part of the chain and to keep getting funds from the boss (be it a senator or the executive director of a funding agency), one must achieve concrete and measurable outcomes that can be spent in political or reputational terms. Because of this reason, the request of innovations and new products coming from the “top rings” of the chain never stops. Actually, bringing to the table a technological prototype in alpha stage is almost always a required precondition for being eligible to a grant.

Yet the problem is that an infrastructure does not only depend on the production of technological innovations, but rather on a patient, timely and steady maintenance work – something which is certainly not that attractive for funders. The example brought by TD1 is clear. In order to release an up-to-date, secure and high-quality operating system, the Tails team have to synchronize its repositories with a number of other infrastructures that the OS depends on: the latest stable Tor release, the latest Tor Browser release, the software published in the Debian repositories, the one *not* being published in there but still being used by Tails, the packages of the GNOME graphic environment and, last but not least, the latest version of the Linux kernel. All this without mentioning the Tails web infrastructure development and administration, as well as the bureaucratic and accountancy work. Who pays for this work? Nobody. Result? The bulk of the infrastructural work – which is essentially invisible because it is intended to keep the system functioning and not to produce changes a funder can brag to her direct superior – is delegated to the good will (and probably to the nightly, unpaid efforts) of those participating to the project. This dynamics potentially undermines the implicit benefits of the open source projects. Without funding dedicated to administration, usability improvement or bug hunting, no system can claim to be secure, no matter the license under which it is released. And, without security, neither privacy nor anonymity can exist.

5.10. How grants shape the infrastructure

There are other reasons because open grants play an ambiguous and contradictory role within Tor. As we have seen, they have a positive impact, because they allow to hire full time employees and pay them a salary. Moreover, they allow the Tor Project to openly operate: since grants are public money, Tor does not have to subscribe any clearances and is free to publish the financial reports every year. But on the other hand, a milestone-based funding model does not seems to be suitable for maintaining an infrastructure which, by definition, along with ‘rigidity’ – that is to say standards, shared elements in order to permit data exchange and collaborative work between different systems on a wide geographical distance – requires ‘flexibility’, namely the possibility of customizing and tailoring technology for local needs (Star and Ruhleder 1996). And this is even more true for an infrastructure being developed according to the chaotic and recursive approach inherent to the open source software development methodology. In plain words, the rigidity of bureaucratic standards that need to be accomplished in order to win a public grant, seems to clash either with the creativity and the degree of freedom required by hackers and activists involved in the building of the infrastructure.

This problem has been explained in 2016 by Moritz Bartl, founder of the Torservers’ organization. During one of the events[27] organized by the Center for the Cultivation of Technology (he is a fellow), the hacker clearly explained how in the Tor Project the joy of writing software is always preceded (and somehow stifled) by a huge investment of time and energies in writing grant proposals.

> "Just submitting 50 or 150 pages, very specifically outlining what do you do with that money, tight that money to specific deliverables, and on the other hand you work with activists that want to pick their own priorities”.

These words closely recall those pronounced in 2015 by Shari Steele during the State of the Onion[28]. Just pinned to the new role of Tor executive director, Steele turned in front of an enthusiast audience describing the goals she wanted to achieve during her office. The first one was the creation of a proper safety net for TPI employees, namely a support system for bank accounts, health insurance and so on. The second was the diversification of funding:

> “the government funding has been so difficult for us because it is all restricted and so it limits the kind of things we want to do. When you get the developers in a room blue-skying about the things that they want to do it is incredible! Really really brilliant people who want to do great things! But they are really limited when the funding says they have to do particular things”.

It is worth noting that the strictness of the grant assignation process affects the form of the infrastructure. Indeed, writing a grant proposal requires a huge amount of energy and time. Before starting a draft, an engineer usually thinks about three or four projects she would like to work on. However, at some point, she will have to choose among one of these projects, since the idea of crafting three or four proposals is simply unfeasible. And what is going to be the most relevant criterion driving her choice? Obviously, whether or not somebody can be interested in funding it. As KM told me:

> "This is something I would like to do but there is no funding for that; this is something which is useful but not so great. However, the funder is definitively interested in it. Hence this is something you are going to do".

Because of this dynamics, developers and hackers are often inclined to work on projects which are most likely to be funded, but they are not necessarily the most relevant for Tor. For instance, as one of the interviewees told me, Tor has been working only on pluggable transports[29] (PT) for a lot time, since funders seems to be mostly interested in the development of these anti-censorship technologies. On the contrary, none of them has among its priorities the improvement of the anonymity features of the network[30]. Again KM:

> "Do not get me wrong, this is still a good thing, it is still useful for people but if had to choose what I want to work on tomorrow, it might not be PT. I guess PTs are not very attractive to the user in the US but are more important for those who live in China. But the point is that, while we are developing these great technologies, Tor can be theoretically targeted by T/A attacks which can be used for deanonymising user. And onion services still present lot of vulnerabilities".

Fabio Pietrosanti, founder and director of Globaleaks, confirms that the problems exist in such terms. Naif (this is his nickname) emphasizes how the political choices at the heart of the Tor funding system have favored the development of certain features of the infrastructure at the expense of others. Particularly, the amount of money allocated by US institutions to favor the development of censorship-bypassing technologies is definitely more than that disbursed for improving anonymous communications tools.

> "In my own view, there is a bias in the allocation of money. And this bias has been affecting Tor for years. Tor was born as an anonymity technology. However, in the latest years the bulk of the funding it got with regard to the Internet Freedom Agenda is about censorship bypass. The reason because onion services are underfunded is that they are of little use for anti-censorship. If one observes how DRL's funds are distributed, it is easy to notice how their biggest share goes to anti-censorship, definitely not to Tor. These tools do not embed the cypherpunk ideal, according to which there is no anti-censorship without anonymity. To put it in another way: the various tools that exist and provide censorship bypass in authoritarian countries work better than Tor, but they do not provide anonymity. It is about private servers and controlled-distribution software. This stuff works and it gets more money than Tor. Tor is well-known in the West, it is the talk of the town. But if we talk about anti-censorship… well, other software work better".

It is worth noting that users who employ anti-censorship technologies in order to connect to Tor are not that many: at the moment I am writing they are more or less 50000 per day (the whole Tor user base is made by 3 million of people). The problem here is that with this funding model the Tor Project has very little leeway: there are few funders who provide money being tied to specific goals. The fact is that such goals, even though they are not unilaterally dictated by a third party to TPI , they are not even entirely set by it. Moreover, it is certainly true that such funders do not influence directly the code written by Tor developers, but at the same time their financial support is motivated by specific political interests – that is to say, the promotion of the Internet Freedom Agenda – which do not necessarily match those of Tor.

5.11. How grants affect developers lives

But that is not all. The scarcity of the funders, their lacking of diversity and the way money is distributed also affect the public communication of the Tor community and its internal discussions as well. And, once again, this problem has been openly admitted by some of its core members during public events and private interviews. “I could go up and I could say a lot of outrageous things, but some of our funders might wonder if they should keep funding us after that” Roger Dingledine asserted in 2013 during the CCC in Hamburg[31]. In other words, here we are in front of a paradoxical situation: the current funding system which, as we have seen above, in the last years has provided a huge amount of money in order to improve the network anti-censorship features seems to be the reason of the emergence of a self-censorship dynamic within its community of developers and volunteers. In 2018, this dynamic seems to be still there, as a person who asked to remain anonymous confirmed during a long chat we had:

> “One issue, with centralization of funding is a self-censorship problem: we do not talk about this things openly [because we are afraid these agencies can take our funds away]. And this is a problem! We pretend that they do not have influence on us: self-censorship is an influence. We can’t criticize them effectively. But it is still true that almost science and technologies are not able to find a funding that is not connected to the US government”.

Furthermore, the lack of fundings and the strictness in their delivery is considered by some interviewees as a possible destabilization tool which could be employed against the community. As Alison Macrina states:

> “There are ways that if you rely entirely on a particular kind of funder, they can manipulate your work in other ways, even if this is not their intention. Not like “You must put a backdoor” but because the way they fund us is so chaotic that they make us have crazy deliverables in very short spans of time that make for a lot of stress. If I wanted to destabilize Tor I would just cut out the money”.

Another problem, being inherent with the funding system, is that it makes Tor vulnerable to the contingency and uncertainty of the US political climate. Yet, most of the interviewees disagreed on this point. Indeed, they asserted – and they are absolutely right about this – that they are not receiving money directly from the US government but by a multiplicity of entities which are tied, but at the same time independent, from it. “The US government is not a monolith” told me Nix, who a few times has got grants from some US agencies. “It is made by thousands of people with very different agendas. It is a presidential government but there is not a strong direction between what is done at federal level and what is done by different departments”. A similar opinion has been expressed also by a TD2 who claimed that this dynamics is coherent with “the way a government, particularly a big one, is in these ages. It is not a single subject or entity that would have one single plan and acts consistently. It is more like a sum of tensions, relationships and power. Different people want different things”. Or, as Alison Macrina pointed out in really plain words, “the US government is so big that within it you can find people interested in funding us and people interested in destroying us”. Yet, the problem remains and the cuts made by the Trump administration in relation to climate change policies seem to be clear warnings in this perspective[32].

Open grants seem to be an element capable of affecting not only the internal organizational processes of Tor, but also the shape and qualities of the network itself. On the one hand, the openness of the code does not make possible to hide a backdoor into it (nor to force a developer to do it). Yet, on the other, the semi-centralization of the funds (the money is coming from few entities, almost backed by the US government) and the way they are obtained and distributed definitely represents a subtle, but significant, form of influence exercised by few actors over the infrastructure. Is it possible to solve these problems? And how?

5.12. Alternative forms of sustainability/1

Right now there is not yet a definite answer to the previous questions, but undoubtedly Tor is trying to put in place several strategies in order to mitigate the problems resulting from the present funding system organization. I will just briefly list them, because I am referring to experiments in progress and, in spite of the first milestones reached, it is still too early to say they have been successful. In fact, we need to consider that these attempts, being implemented from different perspectives, either try to confront with the structural limits of the open source culture (succeeding in some cases, in other cases ending up replicating its consolidated dynamics) and to rejuvenate the organizational practices, deeply entrenched and taken for granted within the community itself. Let us see what they are about.

Firstly, Tor painstakingly worked to a diversification of its revenues, reaping the first benefits of this effort in 2016 and 2017[33]. The 990 forms referring to this two-year period clearly speak and tell that the amount of funds provided by the US government dropped from 85% in 2015, to 76% in 2016, to 51% in 2017. It is a first step forward, made possible by the contribution of private companies such as Mozilla and DuckDuckGo (who benefit in various ways from the technologies being produced by Tor Project and, because of this, are interested in keeping its ecosystem healthy). Certainly, it is not yet the perfect solution, as instead it could be that of getting money completely untied to the desires of any player, either a corporate or governmental one. Yet, also in this perspective, significant steps are being made: the size of the individual donations collected in 2018 amounts to a total figure of $460.000[34]. Right now it is difficult to say whether Tor Project will be able to maintain such a diversification of its revenues. What it is certain is that, if such trend is confirmed, it will definitely ensure a more balanced development of the infrastructure, without some of its components being sacrificed for the sake of the Internet Freedom Agenda.

Secondly, there were considerable efforts in raising the diversity of the organization and defeating its mono-cultural tendencies in the last four years. Tor Project started to hold its biannual meetings also in Global South countries (such as Mexico, whose capital held one of the Tor meetings in October 2018[35]). Tor meetups are being organized in countries such as India[36], Brazil[37] or Chile[38] that, until a few years ago, were out of the range of the organization. After the Appelbaum scandal, the board of directors underwent a deep transformation. By now, seven out of eight old members were replaced and five of its representatives are women. Moreover, among the directors, now there are BAME people whose cultural and ethnic background is neither European nor North American (such as Ramy Raoof[39] from Egypt and Nighat Dad[40] from Pakistan). It is also important to mention that in November 2018, after serving three years as executive director, Shari Steele resigned. Isabela Bagueros stepped in in her place[41]. Latina civil rights activist, participating in Tor since 2015 as Project Manager and UX team leader (as we have seen, the laboratory where Tor has experimented in a most radical way with the concept of diversity), former collaborator of the Brazilian government with regard to several FLOSS projects, Bagueros was a Twitter executive as well (this was when the company was growing from a simple start-up to become one of the global ICT giants). Also, in the last two years Tor Project has opened several positions aimed at opening the community's doors to those categories which are usually underrepresented in the ICT world[42], such as "women (cis and trans), trans men, and genderqueer people", as well as "Black/African American, Hispanic/Latin@, Native American/American Indian, Alaska Native, Native Hawaiian, or Pacific Islander".

Finally, in September 2020 Tor launched a Membership program[43] involving a few private companies whose products and services rely on the onion routing protocol in various way (that is the search engine DuckDuckGo, the antivirus firm Avast, the VPN provider Mullvad, the security computers manufacturer Insurgo and the ISP provider Team Cymru). The aim of this program is providing Tor Project with a more diversified and unrestricted funding sources, so that to overcome the slowness typical of traditional grants. Will these initiatives be sufficient, in order to produce that diversity and inclusion missing until now (in Tor in particular and in FLOSS in general)? Moreover, it is legitimate to ask – and I do not have data to answer this question – whether the diversification of gender and nationality that was recently produced is going to be matched by a class diversification as well.

5.13. Alternative forms of sustainability/2

Also, it is worth noting that some projects affiliated with Tor are trying to become self-sustainable by creating new market sectors whose most important players are ethical firms providing Tor-based services. In this perspective, the whistleblowing platform Globaleaks has had a pioneering role and its experience is worth of some insight. The project was born between 2010 and 2011, during the outbreak of the so-called Cablegate and the release of the whole DoS's diplomatic database by Wikileaks. Founded by Fabio Pietrosanti, Claudio Agosti, Arturo Filastò and Giovanni Pellerano, the group aims to address an evident limit of the organization run by Julian Assange, that is its high degree of centralization that made it vulnerable to attacks carried out by powerful actors. In order to address this problem, the group of hackers created a decentralized platform in which the whistleblowing process is made extremely simple. Anybody should be able to easily report information about corruption, bribes or felonies and disclose them to the public: not only hackers being concealed behind seven proxies, equipped with cryptophones and gifted with superpowers, but also citizens, employees of public and private bodies, activists, public officers. Because this can happen whistleblowing must become mundane, boring, reproducible and, therefore, effective. At first, OTF supported the core development of the platform with two grants. Yet, the third one – once again provided by the DoS funded institution which until now has donated the overall sum of $600.000 to the project – was disbursed with a new and different goal in mind. Indeed, Globaleaks was not asked to develop a new platform feature, nor to reach the nth technical milestone but rather to plan and realize an organizational transformation in order to take the path of financial self-sustainability. The organization developed a business plan in order to survive without relying on the support of the US institutions anymore. Globaleaks then reinvented itself as SaaS (acronym of 'Software as a Service') and changed its vision. Now the goal is not just to enable whistleblowing but, as Fabio Pietrosanti tells me, "to enable the enablers, to enable those who will enable someone else to do whistleblowing". Just like Wordpress can be used by any provider in order to offer its users a blogging service, Globaleaks can be used by Global Voices or Transparency International so that they can offer their audience a whistleblowing service. But how is sustainability engineered into this mechanism? Where does the income for the Globaleaks developers come from? The answer is that there are different possible revenues. First and foremost, these latter can result from a typical GNU Economy business model: an X company creates a service and releases it as free code, an Y customer using it pays a fee to the X company for consulting services.

> "Let's make an example. The Hague International Court of Justice: €20.000 for a leak-collecting project about human rights violations in Libya. The Sole24Ore economic daily? It will provide €7.600 in the first year and €3.500

> each following year. The Municipality of Verona? It will provide €3.500 per year".

But Fabio's vision is definitely more ambitious. The choice of releasing Globaleaks under a GPL3 license, as well as making both its code and documentation accessible, was not only laid down by ethical reasons but also by corporate ones: "we work so that other replicate our own business model" Fabio says. "Right now there are 12 societies in the world that provide Globaleaks-based services. In 2020 I want them to be 100". If a new market sector emerges and is populated by companies providing whistleblowing services based on Globaleaks, Naif's creature cannot but reap benefits from this dynamic, as he openly acknowledges. Becoming the standard for a new ecosystem, as well as a gateway towards other ones (for example the Tor Project), would necessarily ensure "an important revenue. Globaleaks would be the privileged player of this environment, since we created the software upon which it is based". The conditions for this to happen are all present. In the latest years whistleblowing became a consolidated practice in Western newsrooms: having a platform to receive anonymous tips is becoming as obvious as having an email address for getting in touch with somebody. Moreover, in some countries (such as Italy[44]) the law establishes that public administrations and private companies must have appropriate procedures and technical tools able to guarantee the reporting of potential irregularities or criminal and administrative offenses.

5.14. Security through imaginary

"The problem of on-line privacy is very abstract: we need to make it visible if we want to solve it. Communication is crucial"
Nix

Rule number zero of infrastructural studies: infrastructure is by definition invisible. It is an object that somehow resembles a black box: at first sight it is not attractive, it does not turn any curiosity on, nobody wants to look inside it (often it is not even possible to do it), nobody knows what it contains, who built it, or why. It is just there. Day after day, year after year (sometimes, century after century) it marks daily life, it becomes part of the landscape and, progressively, it merges with it until it disappears. We take it for granted so much that we remind of its existence only when it breaks down.

This rule does not apply to Tor. In fact, the aesthetic of a low-latency anonymous network and the imaginary it creates are among its most important security properties. In order to understand why, it is sufficient to dwell for a moment on the fundamental principle that governs the onion routing protocol. The effectiveness of Tor – and therefore the possibility of defeating traffic analysis – increases *pari passu* either with the number of people who participate to the network and the growth of their diversity. As we have seen, because this can happen the community tirelessly works on the usability and sustainability of the infrastructure with the aim of breaking down those invisible barriers that make it less accessible and, therefore, less efficient. Yet this is not enough. Even the visible aspects of the infrastructure – such as the kind of feelings it produces, the imaginary it is associated with or the way it is perceived – can represent an hurdle to its use, to its adoption and, therefore, to its capability to achieve the purpose it was conceived for. This is a problem that since the early stages of Tor's history was theorized. Back in 2004, Dingledine, Mathewson and Syverson acknowledged the possible negative consequences of an illicit use of the network, claiming that

> “when a system’s public image suffers, it can reduce the number and the diversity of that system’s users, and thereby reduce the anonymity of the system itself. Like usability, public perception is a security parameter” (10).

It is worth noting that at the time this idea was utterly hypothetical. Indeed, in the period of its experimental deployment, being occurred between October 2003 and May 2004 (date of publication of the design paper), the public perception of Tor was almost null and no abuse complaint had been issued against volunteers running the network relays. This was because of several concurring factors. First: the very first users of the network were, as argued by Dingledine and Mathewson in a paper published in 2006, “a small number of fairly sophisticated privacy enthusiasts with experience running Unix services that wanted to experiment with the network” (Dingledine and Mathewson 2004, 6), not certainly hordes of script kiddies aimed at making trouble. Second: since its first beta releases, Tor had introduced a restrictive policy that prevented exit nodes from making any request on port 25, the one usually employed by the Simple Mail Transfer Protocol (SMTP). The objective of this technical measure was to prevent the network from being used for massive spam submissions. The occurrence of such a circumstance not only would have affected the performance of the infrastructure[45], but it would certainly have cost it the infamous brand of "rogue network", with the consequent risk of seeing its reputation, its anonymity set and, therefore, its effectiveness compromised. Third: by following this logic and by thinking in a long-term perspective, Dingledine, Mathewson and Syverson had refrained from promoting Tor among digital communities involved in “illicit” activities (or, at least, usually being considered as such):

> “Even though having more users would bolster our anonymity sets, we are not eager to attract the Kazaa or warez communities we feel that we must build a reputation for privacy, human rights, research and other socially laudable activities” (Dingledine et al 2004, 13).

However, once this initial setup and tuning phase was over, Tor started to grow. It did at a pace that went far beyond its creators’ expectations. In fact, when in February 2005, Dingledine, Mathewson and Syverson uploaded the first Tor Tech Report on-line[46] – a document, jointly published by Tor and the NRL’s CHACS, in which the authors detailed the challenges faced up during the network boot stage – they made a prophecy that, in a few years, will prove to be blatantly wrong. While being pleased with the increase of users and relays that they had observed until then, the three hackers claimed that the infrastructure would never have grown beyond a certain limit: "Tor is running with hundreds of nodes and tens of thousands of users, but it will certainly not scale to millions” (Dingledine at al 2005, 14). Nowadays there are between 2 and 3 million Tor daily users, while relays and bridges are almost 9000. There have been many factors which have contributed to the network expansion over the years: among these, the unquestionable technical competence and dedication characterizing the Tor team, the financial base on which it could rely, as well as the network of relationships that it has been able to create (especially in the academic environment). Yet, there is another element that must be taken into due consideration to understand the infrastructure growth rate, namely the increased media visibility enjoyed by the project, also being due to important historical events – such as in 2013 the scandal provoked by Snowden's revelations, the Arab Springs in 2011, the revolts in Iran in 2009, the implementation of increasingly restrictive policies being issued by several states and being aimed at regulating information, which have often put onion routing at the center of the international public debate. On the other hand, in 2006 the very same Dingledine and Mathewson put the increasing number of network users in direct relation with the growing journalistic coverage of Tor:

> “As the project gained more attention from venues including security conferences, articles on Slashdot.org and Wired News, and more mainstream media like the New York Times, Forbes, and the Wall Street Journal, we added more users with less technical expertise” (Dingledine and Mathewson 2006, 6).

In fact, Tor's popularity is also proved by the immense, albeit incomplete, archive of journalistic articles uploaded on the project website[47]. It contains thousands of news published since 2004 which recall many of the fundamental steps that have marked the life of the infrastructure. The attention with which these stories have been preserved and collected over time is not a mere sign of narcissism, neither it is a trivial celebration of the goals achieved by Tor Project, nor it simply represents its chronicle. Indeed, the "Press" section of the site has a meaning which goes far beyond the creation of a collection of positive stories that can be consulted by curious Internet users (maybe to encourage them to use Tor). An article being published in an international newspaper (like the New York Times, the Washington Post, the Guardian or Le Monde, just to name a few) or a service broadcast in prime time on a global television network (such as CNN, BBC, Al Jazeera or Sky) are not only useful to talk to a wider audience than the Tor Project blog could reach, nor they should be considered as a simple set of instructions to explain to a generalist public how to get around censorship or protect online privacy. This type of content has another and more important meaning: as a matter of fact, it confers Tor a role and a positioning within the agenda setting (namely, the list of topics that the media consider as relevant for the public opinion), thus implicitly sanctioning its legitimacy within the current political system. The Tor Project’s website ‘Press’ section is therefore a message itself that, Philo would say, communicates how Tor is fully located "within political and cultural assumptions about what is normal in society" (1990, 5). It is worth remembering that the function of media is not much (or at least not only) to produce contents which are measurable in terms of impact on the public opinion, but rather to fuel a process of cultural and political reproduction through which the legitimate limit, the fence of values, of a given era is defined and within which the political actors belonging to it are supposed to act. In order to ensure itself this legitimacy, to be wrap of this aura of normality, Tor depends on other infrastructures, not only on the technical level but on that of the imaginary one as well. In this sense, the media system is a component of the infrastructure and fully affects its ability to perform the tasks it was created for.

5.15. Coexisting imaginaries

There is a number of reasons because this is true, many of which have been theorized by Dingledine, Mathewson and Syverson between 2005 and 2006. The first one is that media can influence users' expectations about a privacy system. As we know, an anonymous low-latency network becomes more secure when the number of its participants increases. However, because this can happen, it must be perceived as safer and more usable than its competitors. It is worth noting that, it is not necessary that it is effectively true, it is enough that the public thinks it. Sometimes all it takes to unleash social networks and attract attention from traditional media is a sensationalist service being broadcast at dinner time or an article with a pretentious headline being trumpeted on the front page of a prestigious newspaper (like "BfR33. The new bomb-proof network for everyone. Freedom hackers challenge the NSA"). Actually, in addition to the catchy name, BfR33 also presents several technical flaws (such as a bad implementation of some obsolete cryptography libraries), none of which the public is aware of. Does all this matter? Not necessarily because, after being under the eye of the spotlights, BfR33 attracts a certain number of new users and, given the growth of its anonymity set, it becomes safer than its competitors (despite these latter present superior security features). It is a mechanism that creators of Tor do not hesitate to define as “perverse”, but which cannot be dismissed:

> “over-hyped systems (if they are not too broken) may be a better choice than modestly promoted ones, if the hype attracts more users” (Dingledine and Mathewson 2006,8).

This dynamic results in a rule that it is important to follow when designing a security system, that is to say:

> “Security depends not only on usability but also on perceived usability by others, and hence on the quality of the provider’s marketing and public relations” (ibidem).

However, there are other dynamics which refer to the media system and affect the infrastructure security level. For instance, along with user expectations, the public reputation of a network plays a fundamental role as well. Dingledine and Mathewson (2005) identify the concept of reputation with the network users’ social identity and the values usually associated with it. Describing Tor as a network being employed by cancer survivors in order to research information about their medical condition is a thing. Creating the perception of it as a training camp for script kiddies or a virtual square for drug traffickers is a horse of a different color. With this kind of fame it is difficult to imagine that anyone could even get close to the infrastructure, let alone using it on a daily basis. And fame is everything for a network whose effectiveness is directly proportional to the number of people participating to it. First, because, as Dingledine and Mathewson explain, “a network that is always about to be shut down has difficulty attracting and keeping users, so its anonymity set suffers” (2006, 8). Second, "a disreputable network attracts the attention of powerful attackers who may revealing the identities of all users to uncover few bad ones" (ibidem). If users of a privacy-oriented network are perceived as being usually involved in illicit traffics (or, for some reason, they are considered as such), using such network in order to increase security or privacy could be a mistake. The risk is that of ending up with one’s home IP in the blacklist of a law enforcement agency and being subjected to unjustified attention. Third, a bad reputation is not a problem just for the anonymity set extension but it also affects negatively the basis of volunteers who donate machines, bandwidth, time and money to keep the network working.

> “More people are willing to run a service if they believe it will be used by human rights workers than they believe it will be used exclusively for disreputable ends” (Dingledine et al 2005,6).

It seems almost a paradox, but in a network like Tor, privacy and reputation, intimacy and publicity, transparency and opacity, visibility and invisibility must coexist and combine reciprocally, as if they were opposites that attract each other. How this can happen remains an open problem, since, the trio of engineers writes, “the good uses of the network [...] are typically kept private, whereas network abuses or other problems tend to be more widely publicized” (ibidem, 6). Nevertheless it is a problem that permeates a crucial political dimension for Tor and that can be summarized as follows:

> “The Tor Project’s image with respect to its users and the rest of the Internet impacts the security it can provide” (ibidem, 5).

5.16. How media (unwittingly) strengthen online censorship

And it is not over here. When Tor is called into question for bypassing online censorship – a function that, it is worth recall it, Tor was not originally designed for – things get even more complex. Indeed, according to Dingledine (2010) in this kind of scenarios media attention play an ambivalent and, in some cases, openly negative role. Indeed, a censor does not only block technically sound networks but also attack those ones enjoying a great media coverage. If people start catching on the idea that using such tools to escape censorship is a breeze, then the most powerful weapon available to the censor gets jammed, namely its capacity to

> “creating an atmosphere of repression so people end up self-censorship. Articles in the press threaten the censors’ appearance of control, so they are forced to respond” (Dingledine 2010, 6).

According to Dingledine, it follows that one of the ideal features for a censorship circumvention system is that of not promoting itself as such. Better yet, not to promote itself at all: "as long as nobody talks about it much, it tends not to get blocked" (ibidem, 6). In short, if somebody talks too much about an anti-censorship network, it stops working. Yet, if nobody talks about it – and therefore no one is aware of it – it has no reason to exist. There is also a further complication that must be taken into account. As shown in the previous paragraphs, advertisement and marketing play an important role in the funding chain. Indeed, the funders crave positive media attention: they bring it as dowry to their bosses as proof of the goodness of their programmatic choices. Furthermore, public exposure increases the possibility of receiving new funds in the future. It is not difficult to understand why this dynamic is particularly important for Tor. In the framework of the Internet Freedom Agenda promoted by the US government, it has been precisely the development of anti-censorship technologies that has brought a constant inflow of money into its coffers. And yet, this very type of perception and promotion of onion routing risks to undermine its functionality as censorship circumvention system (and therefore eliminating the reasons that lead some of the funders to subsidize the network). Here come again the paradox mentioned a few lines ago. In Tor, fame and stigma coexist, they are two sides of the same coin, they play one against the other, building a piece of the net that, at the same time, risks to destroy it. How to get out of this *impasse*? How to find a balance between obfuscation and visibility? Dingledine's suggestion is "to position the tool in a different context – for example, we present Tor primarily as a privacy and civil liberties tool rather than a circumvention tool" (ibidem, 6).

5.17. Demystifying the 'dark web'

The imaginary that is produced around Tor – the way it is perceived and the concepts people (be them users, funders or politicians) associate with the infrastructure when they are thinking of it – is a crucial component of the infrastructure but, at the same time, it is largely outside the control of Tor Project. Despite their regrettable popularity, concepts such as 'Dark Web' or 'Dark Net' lack any scientific basis, nor they have any pertinence to the technical functions performed by the infrastructure (encryption, authentication, confidentiality, anonymity and reachability). The idea that Tor is used as safe haven by terrorists who are secretly plotting to overthrow their governments has never had confirmation in reality. The hypothesis – lacking in substance but still capable to find room on several online media and in a few controversial libels – according to which Tor would be a giant honeypot devised by US secret services, is little more than bad science fiction, suitable, perhaps, for the trivial plot of a b-movie. Yet, although these imaginaries do not reflect in any way the Tor Project's mission, they are potentially able to compromise the purposes the network was designed for. This is what Roger Dingledine claimed in an interview released to Politico in 2015[48], when he said that he could imagine "a failure mode [of the Tor network] where ... Tor has been smeared so thoroughly so that everybody knows that anonymity is so bad for people". In other words, the dark web imaginary could have self-destructive properties, capable of burying the same infrastructure which has engendered and made it possible. The fact that for Tor it is essential to negotiate its own meaning with the media system also emerges from another statement issued by the security philosopher to Wired USA in 2013[49]. On that occasion, Digledine stated that the NGO he led was constantly "in a war" or, more precisely, in "a conflict of perception. There are a growing numbers of people who are learning about Tor, not from our site, or these talks, but from mainstream newspapers". Even among the people I interviewed, there was somebody who described the link between media representation and Tor using a similar vocabulary. Hellais, for example, referred to it using the term "battle". By telling me about the "massification process" that has affected the hacker cultures over the last 10 years, the activist focused precisely on how this has led to an ambivalent transformation in the relationship with the press.

And this battle is really felt as crucial inside Tor. The proof is that there is an infallible method to piss off any TPI employee or Tor core people. Just refer to the infrastructure with two magic words: 'dark web'. This is certainly a very popular expression that however, as Kate Krauss (a media expert hired by Tor in 2015 to take care of the organization's public relations) pointed out to Daily Dot, "colors negatively the way people think about what we're doing"[50]. I had been able to verify the validity of this statement more than once during my PhD. Whenever I discussed my research project with students and colleagues who did not already have a previous knowledge of Tor, nor some specific training in the field of computer security, the reaction was more or less always the same: “Cool man! The dark web! Silk Road, innit’? Mmmh… that’s not legal fam! How are you going to deal with your ethics?”.

Tor Project tries to systematically oppose the use of this terminology, by demystifying its meaning every time its members take part to a public event, be it a small workshop held in a university classroom, a live TV show or a huge hacker conference. As, for instance, the DEF CON[51], globally being considered as one of the most important meeting for security hacker. Every August thousands of experts, journalists, government officials, spies and lawyers head towards Las Vegas to follow talks and seminars about computer and hacking-related subjects, as well as cybersecurity challenges. Held for the first time in 1993, over time DEF CON has become a mainstream event, followed live by the specialized press. Making the mark over these stages means having access to a huge megaphone. It is no coincidence that in 2017, when he was called to attend the 25th edition of the event and present the next generation onion services[52], Roger Dingledine took advantage of this global proscenium to send a strong and clear message (which would then bounce on hundreds of technological newspapers, blogs and sub-reddits): "the dark web does not exist".

> “Whenever you see a journalist trying to show you the picture of the deep web […] or dark web, think about what they are trying to sell you, because there is basically no dark web, it basically does not exist […] Whenever somebody shows you the picture of the iceberg, try to figure out what their incentives are, what their motivations are”.

5.18. Transparency and its ambiguities

The relationality of the imaginaries characterizing Tor must always be treated with extreme caution. In fact, an object that for somebody is a means of connection, a bridge, for somebody else is an hurdle, an insurmountable barrier. It is an assumption that should never be forgotten. The consequence could be the incommunicability of the infrastructure and the danger of having, metaphorically speaking, one, maximum two men touching the body of the elephant. This could be a critical risk for a network whose functioning entirely rely on the number and diversity of human beings who voluntarily choose to participate to it. Let's think about the idea of transparency, so crucial for the FLOSS movement in which Tor has its own breeding ground. As we know, this multifaceted concept is understood according to a plurality of meanings that are different and, at the same time, complementary to one another. First and foremost, transparency is an operational concept, being synonymous of openness of the source code, that is the precondition that guarantees its inspection and, therefore, the possibility of fixing any bug present therein. Second, transparency is also a concept underlying the Kerckhoffs' principle, from which the whole notion of "security-by-transparency" originates. Formulated in 1883 by the homonymous Dutch cryptographer, this precept states that an encryption system must be considered safe even if all its components – in the case of Tor, its code – are entirely public. Third, transparency stands for the public dimension of the governance practices used for running the infrastructure (funding sources included) as well. All this in the head of a geek who lived and breathed the GPL[53] is a bond of trust, a form of guarantee about the purposes for which Tor was created, the security of its code and the good intentions pursued by its developers. The fact that Tor is transparent is one of the first and last things that are usually said about the project, as well as one of the most important imaginaries associated with it. There is no anonymity (and actually even no Tor) without transparency. This is particularly true for Tor's operational transparency, that is source code openness. Every time during an interview I asked, in a deliberately provocative and captious manner, if the origin of Tor's funding could not be kind of embarrassing or potentially compromising for the integrity of the project, I always received the same answer: "No, because our code as well as our financials are public. We are transparent". However, there have been some significant exceptions (such as Alison Macrina, Antonela Debiasi and Silvia Puglisi) that have decisively rejected this form of self-representation, expressing a certain criticism towards it. While not denying in any way the operational importance of transparency for the security of the infrastructure, the above mentioned hackers, however, questioned its aesthetic utility. Alison, when invited to speak on this topic, responded in this way:

> “So, first let me say that the way Tor has historically answered this question is really insufficient. What they say is “It does not matter where we get our funding from because it is all open source and is fine”. There are a lot of problems with that. Number one: people do not know what that means. You are speaking to a very tiny audience if you expect people understand how open source how… you know, like with open source everything is fine because you can examine the source code”.

In other words, the language of transparency could be incomprehensible because it is spoken by very few people outside of the Tor and FLOSS microcosms. Furthermore, although it is not questioned that Tor source code should be accessible in order to be examined, it is equally out of discussion that this fact in itself does not mean absolutely nothing for 99.999% of the inhabitants of the planet. Only a few can read it and even less are those able to adequately interpret it and verify its correctness. The transparency of the code is at its best a form of indirect guarantee of its security, because it is necessarily mediated by research groups, specifically funded and organized for auditing small portions of it. Some of the interviewees said that the Tor source code is the one more audited by the FLOSS community after the Linux kernel: I do not exclude this is true but, when I asked them for data that could be useful in order to corroborate this hypothesis, none was provided to me. Furthermore, the fact that the Tor Project daily activities is meticulously documented does not necessarily make it more transparent. 15 years of mailing lists, design documents, technical specs, changelogs, wiki articles, financial statements, transcriptions of IRC chats, notes about the internal meetings, footage of public meetings, posts and comments on the blog: the amount of information to be analyzed and interpreted in order to depict an, even partial, historical slice of life of the community is disheartening, absolutely out of reach for any individual. Moreover, this informative overload is made even more nebulous by the geek jargon that pads out the daily interactions of Tor Project members and, in some cases, becomes almost impenetrable because of the very high technical competence required to extricate itself from within. It is unavoidable since, as told to me by Nathan Freitas of the Guardian Project, one of the minimum common denominators that distinguishes the participants in Tor is their "technical excellence". Without proper knowledge and skills, it is just not possible to make sense of the esoteric discussions that take place in a mailing list like tor-dev. In short, even transparency, as well as open source, seems to be a matter for very few chosen ones.

5.19. The blind men and the elephant

There is one more reason because Dingledine's above mentioned talk is interesting. In the first minutes of his speech, the hacker explains how the concept of diversity does not exclusively relate to the composition of the anonymity set, but it also permeates the processes of representation of the network, that is to say the way in which Tor is "made present" in the eyes of a recipient through a content made of values, perceptions, concepts that characterizes it, thus giving him a form, an external aspect, an aesthetic.

> "I actually only use the word anonymity when I am talking to other researchers. When I talk to my parents and ordinary people I tell them that I am working on a privacy system, because anonymity maybe is scary but privacy is a good value that all world should have. And when I talk to companies, Google and Walmart and so on, I tell them I am working in communication security, because privacy is dead and anonymity is scary but security, yeah yeah, I need some security. And then, when I am talking to governments and military, I tell them that I work on traffic analysis resistant communication networks. And again is the same system, it is the same network, it is the same set of users, it is the same security properties, but the goal is to blend this different sets of user together [...] And another forth category which is reachability or the censorship side".

In spite of its apparent simplicity, Dingledine's reasoning betrays the profound awareness of shying away from any temptation to represent the network with an identitarian aesthetic, a single narrative or a universal imaginary. It is a luxury that Tor cannot afford, since involving a large group of heterogeneous subjects in the infrastructure is the fundamental condition to guarantee its effectiveness. When Dingledine (or any other of the core people) chooses to present Tor using a word like "anonymity", rather than "security", or "privacy", or "traffic analysis" or "reachability", it is never to understood with its mere technical meaning but also, and above all, as a linguistic interface properly configured to bridge and create a connection with a public belonging to a context rather than another. Tor must become an infrastructure from this point of view as well, because, in addition to having to bring together different threat models, it must also be able to catalyze in itself the different aesthetics associated with them. Network security also depends on paying attention to these imaginaries, on cultivating them and communicating the different Tor properties to different audiences, characterized by different expectations and interests. It is a concept that during a YouTube podcast Paul Syverson explained with the Indian fable of the six blind men and the elephant, a philosophical parable about relativism and the value of tolerance[54]:

> “I like to think of it like the all story of the blind men and the elephant [...] One is touching the tusk and says “It is a spear”, and one is touching the side and says “it is a wall”, one is touching the leg and says “it is a pillar”, one is holding the tail and says “it is a rope”, one is holding the ear and says “it is a fan”. The difference is that all these people, you know the law enforcement office, the ordinary citizen, the journalist, the abuse victims, they are like the blind man except that they are not wrong. I mean, it is all these things, but it provides different things to different people, which is actually kind of where it gets its security from, because by providing these values to these different kinds of people it makes it harder for an adversary to know what sort of person is using the network at this time and why”.

6.Conclusions

6.1. Forced to live side by side

I struggle to make sense of the complexity that characterizes the Tor network and that I tried to explore in this thesis. In the first chapter, in order to contextualize the historical and political context within which Tor is situated, I drawn upon the relevant literature in the fields of Science and Technology Studies, Infrastructure Studies, Internet Studies and Internet Governance Studies. In doing so, I paid particular attention to the power relationships that constitute the contemporary Internet and that gave life to a hyper-centralized global network marked by geopolitical tensions, economic oligopolies and widespread surveillance. These topics were crucial for understanding the necessity to engage with Tor and interpreting the politics that its community pursued, as well as analyzing the structures of power and cultural imaginaries embodied into its infrastructure. In the methodological chapter I described the research design, the sites of my ethnography and the key participants of this study. In chapter 3 I focused on the analysis on the Tor's funding system and, in doing so, I have been able to identify some the main production mechanisms of the network. In chapter 4, I examined how the Tor developers interpret the concept of privacy and translate it into the technological artifacts they build. Finally, in chapter 5, I explored a set of politics adopted by the Tor community to optimally configure the infrastructure so that this can achieve the goals it has been designed for.

Summarizing the work done is almost impossible but, if I had to choose a word to start from in order to unravel the tangle of relationships, technologies, histories, protocols and political paradigms that give shape to this infrastructure, then this would be *reform*: Tor is a vast and articulated project of reform of the Internet aimed at rectifying the daunting imbalance of power nowadays afflicting it. I use the term reform in the sense suggested by Coleman, according to whom FLOSS is not just a virtuous process of technological development aimed at the production of free, non-proprietary software, traditionally being considered superior to its closed-source counterpart. On the contrary, as she argues, radical ethics of knowledge sharing and open working methodologies are to be considered above all as elements underpinning a "liberal critique within liberalism" (Coleman 2013, 17), which, while drawing on the traditional theoretical toolbox of liberalism, it puts into questions some of its fundamental concepts in order to reinvent it. Just as the proliferation of copyleft licenses has had the value of stimulating a political and scientific debate about the legitimacy of intellectual property in a world where information reproducibility at no cost has become law, so the popularity of the Tor network has driven its participants to question the adequacy of individual privacy and the limits it presents against the prevalence of digital surveillance that acts on a global scale and reverberates its effects through society as a whole.

After all, as also argued by Kelty, the epistemology of FLOSS is precisely that of a liberalism updated to the 21st century which, through practices of reform and reconstruction, allows not only to challenge established institutions and power configurations, but also to imagine “the chancy making of new beginnings” (Kelty 2013). In this sense, FLOSS underlies a dialectical relationship between past and future which, as we have seen, deeply permeates and informs the Tor network as well. In fact, although the organizational practices upon which it is based have their origins in a multiplicity of alternative political and cultural paradigms – such as the hacker ethics, the cypherpunk imaginary or the free speech liberal culture–, they are considered anything but uncontested by the people who are involved in the management of the infrastructure: on the contrary, as it emerges from my interviews, such practices are object to an intense criticism, symptom of a widespread need for their renewal and adaptation to contemporary times. The painstaking work to improve the user experience beyond US and Europe; the questioning of the centrality of academic research in the software development process; the frantic search for diversified sources of funding to ensure greater independence of the project; the attempts being made to build organizational forms that counterbalance the white male and western privilege that characterizes open source culture; all of these are concrete efforts that show an active commitment taken by the Tor community to renew the FLOSS movement and strip it of a number of power structures that limit its libertatory potential.

And precisely the idea of stripping the Internet infrastructure of a series of technical functions and reassigning their control – along with the power resulting from them – to users is at the heart of the project of technical reform carried out by Tor. Such project consists in rewriting some of the fundamental rules that still today govern the Internet (like the IP) but were conceived in a historical context with completely different characteristics from the current one. In the original intentions of the creators of Arpanet – a small, decentralized network inhabited by a few thousands of people – the IP had the sole function of moving a datagram from one network end to another, in a distributed manner and as quick as possible. Pioneering figures of the cyberspace, like Jon Postel and David Khan, could have never ever imagined that over the years the Internet would have turned into a radically different environment – a global battleground characterized by topographical gigantism, technical centralization and privatization of the public sphere – and that within it routing procedures would have become a source of authority that a handful of actors draw on in order to interfere with the lives of billions of people, by monitoring their daily activities, censoring their communications or analyzing them for profit. Tor's goal is precisely that of depriving the web of such forms of authority through the creation of a voluntary overlay network based on a new routing protocol designed to "make the Internet stupid again", as it had actually been originally conceived. How? By disintermediating a series of technical functions – for instance those of traffic identification, authentication and encryption – that in the onion routing are not being performed anymore by the infrastructure but are directly taken over by clients.

Yet, the work of authority loosening carried out by the Tor Project is not only oriented to the re-conversion of the Internet into a mere carrier, or if you prefer, an oblivious network without firewalls and walled gardens. The activities that the community carries out on a daily basis go far beyond IP bug fixing or the construction of technologies designed in response to the threats posed by digital surveillance. Indeed, Tor not only works to solve problems originating from the past, but it also proved to be an active agent capable to autonomously plan future changes. In fact, the voluntary nature of the network and the practices of limited government it is administered with, make Tor an *in vitro* experiment that implements on a small scale a possible model of Internet

Fig. 14: 2019 Tor fundraising banner

governance which effectively works and, at the same time, is characterized by a very low gradient of authority, that is to say by the presence of a few administrative entities that are endowed with a reduced power by design. One thinks, for example, of the ‘Directory Servers’ whose operation has been briefly described in chapter 1. The power of exclusion exercised by these relays applies only to a very limited number of cases: in fact, the servers which are object of such power are mainly those that run obsolete versions of the protocol (and therefore jeopardize the efficiency and security of the infrastructure) or try to become themselves an authority (namely to interfere with the activities of clients) thus explicitly contravening the main purpose Tor was created for. In no case directory servers could ever exclude a client from the network for the information it publishes or for the information it accesses, and this is because the entire infrastructure has been designed so that no actor, inside or outside of it, is in the position to know who is talking to whom. The authority of the administrative bodies of Tor is weak, because the power that constitutes it is weak and because its exercise is aimed at ensuring that the degree of authority the various components of the network are endowed with remains weak.

Disintermediating therefore means reconfiguring the status of authority on the Internet but also testing the present state of things. It is no coincidence that the slogans chosen in 2019 by the Tor Project to launch its annual fundraising campaign are "Take Back the Internet with Tor" and "A better Internet is possible, I've seen it". But beware: one must not be misled by the cyberpunk graphics or by the 90's Internet culture visual references employed for advertising such initiative. The Tor Project is not a mere restoration of the original rhizomatic order of the network, nor it is the naive dream of a group of nostalgic engineers who yearn for the return of the glories of a bygone time. It is not "what it was", much less "what it will be". On the contrary, to paraphrase Papadopoulos (2018, 174), Tor embodies an idea of the future made up of practices for reclaiming the past and building *now* an infrastructure that can shun the universalizing character of the contemporary Internet: as we have seen in chapter 1, a network of a few administrative macro domains whose owners are driven by the tyrannical ambition to create platforms where to amass as many technical functions as possible and to perform any task (or satisfy any desire) of daily life. Being engineered to attract all forms of diversity and normalize them, the design of these environments produces a collapse of conceptual opposites and a disappearance of the dialectic of negativity: indeed, within them the boundaries between public and private, freedom and subordination, individual and environment, utopia and dystopia, past and future become liquid and fade gradually away.

Tor seems to be the polar opposite of this. In fact, it was born with the aim of materially carrying out a gesture of rupture, that is to produce a dimension of separation – the one between routing and identification – within the only Internet Protocol Suite layer governed by the rules of one single protocol (the IP). In addition, the infrastructure based upon onion routing has been built with the concept of 'distributed trust' in mind: routing confidentiality does not depend on a single relay and none of the components of the network fully know the path followed by a datagram to reach its destination. Furthermore, users' privacy cannot be entrusted to a system owner because this latter does not exist – the infrastructure is under the control of multiple administrative domains, be them technical or legal –, just as there is no subject who can bind the activity of the network nodes to its will: each relay, each client is the arbiter of its own decisions and it cannot become the arbiter of others' decisions. The only authorities being present in the infrastructure are specifically designed to carry out as few tasks as possible and their ultimate goal is to preserve the proper functioning of the network and, above all, its diversity.

Diversity is precisely the concept around which the entire organization of Tor revolves. It is a goal (the inclusion of a plurality of heterogeneous subjects has always driven the development trajectory of the platform), a mean (a broad and varied anonymity set is essential to ensure the efficiency of the infrastructure) but it is also the foundation of the non-written agreement signed between the parties involved in the construction and administration of the network. As Gus, current Community Team leader, told me during an interview "if we deployed a mechanism for arbitrarily censoring bad onion services or we created an authority for providing domain names to the sites on the network, Tor would break down: developers would stop to take part to the project and people would not use it anymore”. The reason because Tor exists and works, he added, is that “I can use it for whatever I want, because you can use it for whatever you want, whether I like it or not”. According the to former leader of the Community team Alison Macrina, with whom I have discussed in depth the Tor’s politics in chapter 5, it is precisely by virtue of this tacit agreement among the people who take part to the life of the infrastructure that Tor has always had the potential to attract “a plurality of political visions, even radical ones, although it was originally inspired by an approach most easily described as liberal-democratic”. And the need to make a plurality of different political views coexist within a single environment has generated by extension a non-vertical organizational structure, within which, the leader of the UX team Antonela Debiasi claimed during the discussion I had with her, “we collectively discuss roadmaps and try to find consensus on what to build next but there is not one person, a top manager, a governing body who tells to other people what they are supposed to do. This kind of leadership does not exist because we don’t have a global shared political vision about what we are doing: there is a lack of it”. In this sense, as Hiro (sysadmin of the Tor Project web applications) asserted by resorting to a beautiful and effective metaphor, the political spectrum of Tor “is a circle. Within it you can find anybody and anything: socialists, anarchists, liberals, libertarians and much more. Each of these political groups is an arc of the circle. At its ends, each arch touches the ends of other arches: their point of contact is a technical property or a feature of the infrastructure they are interested in, often for different reasons. Yet on other issues these groups continue to have quite opposite opinions and practices". The different actors taking part in Tor do not work to create a common political vision but to build an environment suitable to include within it a plurality of alternative forms of life who are forced to live side by side in order to disrupt the power relations that constitute the contemporary Internet, as well as to carry out "the material and practical maintenance and modification of the technical, legal, practical and conceptual means" (Kelty 2008, 3) that make their existences, freedoms and futures possible.

As any doctoral thesis also this work must be considered incomplete. There are many stories, techniques and topics related to the Tor network that I would have liked to study more in depth but which I could not include because of space and time. Continuing this research would involve developing a more comprehensive historical account of Tor, something that was not my primary aim in this thesis but could be a project of its own. For example, one could study evolution of onion routing in the years immediately preceding the publication of the Tor design document published in 2004. Furthermore, given the centrality of concepts such as ‘distributed trust’ and ‘weak authority’, a greater attention should have been devoted to the study of the algorithms employed by the directory servers to elaborate the ‘consensus’ document (the one that defines the network topography on hourly basis), as well as to the policing practices implemented by the community to exclude relays being specifically configured to violate users' privacy. It is a complex job which, however, can be carried out through the study and consultation of the Tor changelog, its manual and, above all, the vast archive of technical specifications progressively included in the onion routing protocol.

However, this thesis has contributed to a better understanding of Tor as power equalizer in the current Internet infrastructure, if possible, also by demystifying a series of imaginaries (such as that of the ‘dark web’) that depict it as a rogue network and are essentially employed by its adversaries to delegitimize it. On the contrary, Tor has to be considered as a reform project born out of liberal values that relies on diversity and aims at producing a technical disintermediation of the Internet and a loosening of the forms of authority online. Yet, this reform spilled beyond liberal tenets and went as far as to challenge liberalism itself, thus attracting to the infrastructure other forms of political commitment and practices. And it is precisely in this heterogeneous composition of the Tor community that it is possible to find the deep meaning of the idea of privacy that this low-latency anonymity network embodies. A concept that lacks an ontological unity and does not have a unique meaning for the participants to the network but that, on the contrary, it alludes to a material configuration of reality where it is once again possible to build a future, or rather many possible futures, sheltered from the tyrannical and universal gaze of digital surveillance.

Appendix A:
Approaches to data research management

In order to protect my research data, I will resort to two established security models in the hacker culture, namely security by transparency and security by compartmentalization. Before starting, I want to stress that the following security models are interwoven and overlapping. They will inform *to the same extent* the creation of my infrastructure of research: if one of them fails, the whole infrastructure will fail.

1. Security by transparency

During my research I will not gather data resorting to any kind of closed-source software: on the contrary, all the information collected will be stored in a laptop running FOSS (Free and Open Source Software). The choice of adopting FOSS as foundational element of my research infrastructure comes from the will of overcoming the security-related problems typical of closed-source software. As a matter of fact, proprietary systems can be secure only as long as nobody outside its implementation group usually a commercial company is allowed to find out anything about its internal mechanisms. Indeed, proprietary software is only released in binary form – readable by machines but not by human beings –, while its source code is not publicly available.

Therefore, the use of closed source software has relevant drawbacks in terms of ethical approach to research:

a) It is impossible engage in an auditing process of the code;

b) When a bug is found, researchers experience a total dependency on the vendor, even for what concerns the release of the patches required to fix dangerous vulnerabilities which can put in danger the integrity and confidentiality of the data;
c) The researchers are forced to put a blind (and resigned) trust in the programs executed on their devices;

In other words, the very nature of proprietary software removes from the root the possibility of knowing how a given program works: without this kind knowledge, there are no *scientific* evidences which permit to state that such program is safe and suitable for the management of sensitive data.

On the contrary, relying on FOSS permits to partly overcome the above mentioned problems:

a) Source code can be audited without any form of technical or legal restrictions;
b) When a bug is found the patching process is usually very fast;
c) The code review is undertaken by a large community of hackers who are not driven by economic interests;

In other words, researchers put their trust in a larger number of actors not a single private company who are moved by ethical concerns.

2. Security by compartmentalization

It is worth noting that the availability of the code is not in itself a guarantee of security. Because of this, I will resort to a second security model, namely security by compartmentalization. The foundational principle of this security model is grounded on the assumption that security measures, as much as they can be refined, always present holes: therefore, rather than focusing on the protection of a whole system, it is much more useful to pursue a logic of harm reduction. If a single target in our case, a single laptop for storing research data is difficult to defend, it makes sense turning and splitting it into multiple targets. This aim can be pursued through a technique called virtual isolation, consisting in the creation of a set of virtual machines (VM) that run inside a computers' main operating system.

A VM can be thought as a computer within a computer. Any single VM can be dedicated to a different specific task: one can be used for storing sensitive research data, one for writing notes, one for surfing the web, one for managing e-mail accounts and so on. A configured set of VM provides an additional protection made of separate operative systems for managing alternate data without having to use multiple computers. [1]

3. Infrastructures: tools

a. Main laptop

- Qubes OS. Although the security by compartmentalization model can seem highly complex in the eyes of the inexperienced reader, it has been recently simplified and made accessible by Qubes OS. Qubes is an operative system which aim is that of keeping the things one do on his or her computer isolated in different virtual machines. In this way, if one VM gets compromised, nothing else will be affected. In my particular case, my interviews and digital research data will be kept in a specific qube/VM (called "vault") without access to the networking stack: in this way, an hostile actor will not be able to ex filtrate the more sensitive data of my research without having a physical access to my machine. For a table of my VM scheme see Appendix A.
- Anti Evil Maid. In order to protect my laptop from physical attacks, I will resort to another mechanism deployed in Qubes OS, namely Anti Evil Maid. As explained by Joanna Rutkowska [2], Qubes Os founder and team leader, "Anti Evil Maid is an implementation of a TPM-based static trusted boot with a primary goal to prevent Evil Maid attacks [...] The adjective trusted, in trusted boot, means that the goal of the mechanism is to somehow attest to a user that only desired (trusted) components have been loaded and executed during the system boot [...] The idea is that if a user can see correct secret message (or perhaps a photo) being displayed on the screen, then it means that correct software must have booted, or otherwise the TPM would not release (unseal) the secret.

Another way to look at it is to realize that Anti Evil Maid is all about authenticating machine to the user, as opposed to the usual case of authenticating the user to the machine/OS (login and password, decryption key, token, etc). We proceed with booting the machine and entering sensitive information, only after we get confidence it is still our trusted machine and not some compromised one". In order to improve the security of this process, my AEM boot partition will be stored in an external USB stick and not in my internal hard drive [3].

- USB Qubes + USBGUARD. Another possible vector of attacks are USB drives. In order to avoid BadUSB attacks happening I will employ two different tools. First, I will manage untrusted USB device with a USB qube. A USB qube is a VM which acts as a secure handler for potentially malicious USB devices, preventing them from coming into contact with the core of QubesOS (dom0). With a USB qube, every time you connect an untrusted USB drive to a USB port managed by that USB controller, you will have to attach it to the qube in which you wish to use it [4]. Second, I will employ USBGUARD. USBGuard is a software framework for implementing USB device authorization policies (what kind of USB devices are authorized) as well as method of use policies (how a USB device may interact with the system) [5].
- Onion Updates. The daily updates of the templates (Fedora, Debian and Whonix) upon which my system is built will be performed, when possible, through onion services, in order to avoid some possible attacks (like targeting my system with malicious packages or Traffic Analysis for tracking the software installed on it).
- Basic measures. Full-disk encryption with AES-XTS-PLAIN64 cipher, complex alphanumeric passwords, BIOS password and anti-tampering BIOS functions. Password will managed with a password locker (KeepassX) and stored in a separated qube/VM (called "work-gpg") without access to the networking stack.

b. Secondary laptop

My secondary laptop will be configured according to the above mentioned security measures.

c. Smartphone

Even though I will not store any sensitive data on my smart phone, I will likely need it in order to conduct interviews. The only reasonable choice in order to pledge my personal security and that of my interviewees seems to be Graphene OS. Based on AOSP (Android Open Source Project), Graphene OS is an operative system for smart phones built with privacy and security in mind. It is compatible with one of my above mentioned approach towards security (security by transparency) and presents several advantages:

- It is completely open source.
- It employs F-Droid as app repository. F-Droid comprise only FOSS software.
- It does not rely on Google Services.
- It delivers monthly Android Security Updates once they are available.
- It supports File Based Encryption (FBE), Trusted Boot, Exec Based Spawning Model and several more hardening features. For a complete technical overview see [7].

d. Voice recorder

Interviews will be gathered with a traditional and connectionless voice recorder.

4. Infrastructures: practices

1. Getting in touch with my interviewees

In order to get in touch with my interviewees I will rely on privacy-oriented e-mail providers which support Onion POP3 and SMTP services. My mail will be encrypted with GPG. My private key (RSA 4096) will be stored on my Yubikey 4. Mails will be downloaded daily and stored on my encrypted hard drive.

2. Interviews

The interviews will feature personally identifying information only with the consent of the participants: even in case of verbal consent, the recording will include only a 'yes or no' sort of response, and the participant identity will be store somewhere else. I want to clarify in advance that I will not ask or gather any information on potentially incriminating subjects. In order to avoid my respondents say anything which could harm them in a court of law, all my interviews will be prefaced with this caveat and all the questions will be structured with this tenet in mind.

I will conduct two types of interview:

- Face-to-face interviews. When possible interviews will be conducted in person. Data will be recorded on the external memory (microSD) of the voice recorder, whereas internal memory is not going to be used. Once recorded, data will be immediately saved on my qube without access to the network and wiped from the external memory of the recorder.
- Phone calls. They will be conducted though Signal. Data will be recorded on the external memory (microSD) of the voice recorder, whereas internal memory is not going to be used. Once recorded, data will be immediately saved on my qube without access to the network and wiped from the external memory of the recorder.

3. Transcription of the interviews and deletion of raw recordings

No external transcribers will be hired: I will personally transcribe all the interviews. Once my research will be over, the original raw recordings will be destroyed resorting through the Gutmann method: this is an algorithm for securely erasing the contents of computer hard disk drives which involves writing a series of 35 patterns over the region to be erased.

4. Sharing of my research data with my supervisors

My supervisors will not have access to the raw audio recordings, nor to their transcriptions. I do not have any legal, professional or ethical duty in this sense.

5. Backups

I will perform four different types of backup.

- The first one will rely on Qubes Os backup system. It will be employed to save my VMs on an off-line, encrypted hard disk. This backup will also include sensitive data (voice recordings and notes about them). It will be performed weekly.

- The second one will rely on Qubes Os backup system. It will be employed to save my VMs from my primary laptop and restore them to my secondary one. This backup will also include sensitive data (voice recordings and note about them). It will be performed quarterly.
- The third one will rely on my domestic OwnCloud setup, running on a network connected RaspberryPI 3. Unfortunately OwnCloud allows only server-side encryption. This backup will include documents related to my PhD research but no sensitive data.
- The forth one one will rely on a WebDav directory provided by a privacy-oriented ISP. Data will be saved and encrypted with Duplicity which supports client-side encryption [8]. This backup will include documents related to my PhD research but no sensitive data.

6. Oversea travels

My secondary laptop will be used only in two circumstances. First, in case of failures of my primary hardware. Second, in case of oversea travels. This latter eventuality is the most problematic. Indeed, in the event of a border security control I could be forced to reveal my password or my laptop could be tampered. In order to avoid this possibility (and therefore the compromising of the gathered sensitive data), I will delete any VM containing sensitive data from my secondary laptop, and restore them with the Qubes OS backup system [6] after my way back.

Links

[1] Tactical Tech Collective. 2015. "Zen and the art of making tech work for you". Accessed September 27, 2020. https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual

[2] Rutkowska, Joanna. 2011. "Anti Evil Maid". Accessed September 27, 2020. https://blog.invisiblethings.org/2011/09/07/anti-evil-maid.html

[3] Qubes-Os. :Anti Evil Maid manual”. Accessed September 27, 2020. https://github.com/QubesOS/qubes-antievilmaid/blob/master/anti-evil-maid/README

[4] Qubes-Os. “Using and managing a USB qube”. Accessed September 27, 2020 https://www.qubes-os.org/doc/usb/

[5] Usbguard. “Homepage”. Accessed September 27, 2020. https://github.com/dkopecek/usbguard

[6] Qubes-Os. “Qubes Backup, restore and migration”. Accessed September 27, 2020. https://www.qubes-os.org/doc/backup-restore/

[7] GrapheneOS. “Homepage”. Accessed September 27, 2020. https://grapheneos.org/

[8] Duplicity. “Documentation”. Accessed September 27, 2020. http://duplicity.nongnu.org/docs.html

Bibliography

Aboba, Bernard and Davies, Elwyn B. *Reflections on Internet Transparency*. RFC 4929. https://tools.ietf.org/rfc/rfc4924.txt

Albanese, Andrew R. 2002. “Cyberspace: The Community Frontier”. In *Library Journal*, November 2002, 41-44

Alberts, David S. and Hayes, Richard E. 2003. *Power to the Edge. Command and Control in the Information Age*. CCRP Publication Series. http://www.dodccrp.org/files/Alberts_Power.pdf

Allman, Eric. 2011. “The Robustness Principle Reconsidered”. In *Communications of the ACM*, 54:8, 40-45.

Anderson, Ross J. 1997. *The Eternity Service*. https://www.cl.cam.ac.uk/~rja14/eternity/eternity.html

Assange, Julian. 2014. *When Google Met Wikileaks*. New York-London : ORBooks

Badialetti, Gianmarco and Giacomello, Giampiero. 2009. *Manuale di studi strategici. Da Sun Tzu alle ‘nuove guerre’*. Milano : Vita e Pensiero

Barbrook, Richard. 1998. “The Hi-Tech Gift Economy”. In *First Monday*, 3:12, https://journals.uic.edu/ojs/index.php/fm/article/view/631/552

Barlow, John Perry. 1996. *Declaration of the Independence of the Cyberspace* https://www.eff.org/cyberspace-independence

Batacchi, Pietro. 2009. *La Network Centric Warfare e l’Esperienza Italiana. Il Processo di Digitalizzazione dell’Esercito*. CeMiSS http://www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/83169_NetCenWarpdf.pdf

Bauman, Zygmunt and Lyon, David. 2014. *Sesto Potere. La sorveglianza nella modernità liquida*. Translated by Marco Cupellaro. Bari : Editori Laterza

Bennett, Colin J. 2011. “In Defense of Privacy. The Concept and the Regime”. In *Surveillance and Society*, 8:4, 486-96

Bennett, Colin J. and Parsons, Christopher. 2013. “Privacy and Surveillance: the Multidisciplinary Literature on the Capture, Use, and Disclosure of Personal Information in Cyberspace”. In *The Oxford Handbook of Internet* Studies, edited by Dutton, William H., 486-508. Oxford : Oxford University Press

Benjamin, Robert S. 1954. *Historical Background of Traffic Analysis*. Memorandum NSA-142K. https://archive.org/details/41705939074525/page/n1/mode/2up

Birkinbine, Benjamin J. 2020. *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software*. London : University of Westminster Press.

Block, Fred L. 2008. “Swimming against the Current: The Rise of a Hidden Developmental State in the United States”. In *Politics and Society*, 36:2, 169-206

Borrmann, Donald A., Kvetkas William T., Brown, Charles V., Flatley Micheal J. and Hunt, Robert. 2013. *The History of Traffic Analysis: World War I – Vietnam*. Fort George G. Mead : Center For Cryptologic History, National Security Agency.

Bowker, Geoffrey C. 1996. “The History of Information Infrastructures: The Case of the International Classification of Diseases”. In *Information Processing and Management*, 32:1, 49-61.

Bowker, Geoffrey C. and Star, Susan L. 1994. “Information Mythology and Infrastructure”. In *Information Acumen: The Understanding and Use of Knowledge in Modern Business*, edited by Bud, Frierman. London : Routledge

Bowker, Geoffrey C. and Star, Susan L. 2000. “Invisible mediators of Action: Classification and the Ubiquity of Standards”. In *Mind, Culture, and Activity*, 7:(1&2), 147-63

Bowker, Geoffrey C. and Star, Susan L. 2012. “How to Infrastructure”. In *Handbook of New Media: Student Edition*, edited by Lievrouw, Leah A., and Livingstone Sonia, 230-45. London : Sage

Bowker, Geoffrey C., Baker, Karen, Millerand, Florence and Ribes, Davis. 2010. “Towards Informaton Infrastructure Studies: Ways of Knowing in a Networked Environment”. In *International Handbook of Internet Research* edited by Hunsinger, Jeremy, Klastrup, Lisabeth and Allen, Matthew, 97-117. New York : Springer.

Boyd, Danah and Crawford, Kate. 2012. “Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon”. In *Information Communication and Society*, 15:5, 662-79.

Bradshaw, Samatha and DeNardis, Laura. 2019. “Privacy by Infrastructure. The Unresolved Case of the Doman Name System”. In *Policy & Internet*, 11:1, 16-36.

Bridle, James. 2019. *Nuova Era Oscura*. Translated by Fabio Viola. Roma : Nero

Burrell, Gibson and Dale, Karen. 2003. “Building Better Worlds? Architecture and Critical Management Studies”. In *Studying Management Critically* edited by Alvesson, Mats and Wilmott Hugh, 177-196. London : Sage

Cacciari, Silvano and Pizio, Daniele. 2015. “Insorgenti Dentro i Big Data”. *Il Manifesto*, July 3, 2015. https://ilmanifesto.it/insorgenti-dentro-i-big-data

Callimahos, Lambros D. 1958. “Introduction to Traffic Analysis”. In *Military Cryptanalitica*, *Part II*, 3:2, 6p. https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/tech-journals/intro-traffic-analysis.pdf

Carlini, Franco. 2002. *Divergenze Digitali. Conflitti, Soggetti e Tecnologie della Terza Internet*. Roma : Manifestolibri.

Castells, Manuel. 2002. *Galassia Internet*. Translated by Stefano Viviani. Milano : Feltrinelli

Cebrowski, Arthur K and Garstka, John H. 1998. “Network-Centric Warfare – Its Origin and Future”. In *US Naval Institute Proceedings.*

Chaum, David. 1981. “Untraceable electronic mail, return addresses, and digital pseudonyms”. In *Communications of the ACM*, 24:2, 84-89

Chepsiuk, Ron. 1996. “Librarians as cyberspace guerrillas”. In American Libraries. September 1996. 51

Clark, David D. 1988. “The Design Philosophy of the Darpa Internet Protocol”. In *Proc. SIGCOMM ‘88*, *Computer Communication Review*, 18:4, 106-14

Clark, David D., Cerf, Vinton G., Chapin, Lyman A., Braden, Robert and Hobby, Russell. 1991. *Towards the Future of Internet Architecture*. RFC 1287. https://tools.ietf.org/rfc/rfc1287.txt

Clark, David D., Partridge, Craig, Braden, Robert T., Davie, Bruce, Floyd, Sally, Jacobson, Van, Katabi, Dina, Minshall, Greg, Ramakrishnan, K.K, Roscoe, Timothy, Stoica, Ion, Wroclawski, John and Zhang, Lixia. 2005. “Making the world (of communications) a different place”. In *ACM SIGCOMM Computer Communication Review*, 35:2: 91-6

Couldry, Nick. 2015. *Sociologia dei Nuovi Media. Teoria Sociale e Pratiche Mediali Digitali*. Translated by Virginio B. Sala. Milano-Torino : Pearson

Coleman, Gabriella E. 2004. “The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast”. In *Anthropological Quarterly*, 77:3, 507-19

Coleman, Gabriella E. 2008. “The Hacker Conference: a Ritual Condensation and Celebration of a lifeworld”. In *Anthropological Quarterly*, 83:1, 99-124

Coleman, Gabriella E. 2010. “Ethnographic Approaches to Digital Media”. In *Annual Review of Anthropology*, 39. 487-505

Coleman, Gabriella E. 2013. *Coding Freedom. The Ethics and Aesthetics of Hacking*. Princeton-Oxford : Princeton University Press

Cooke, Thomas N. 2015. *(Re)Configuring Security*, *Power and Privacy: Circumnavigating Conceptual Conundrums through Dissent Anonymity Software*. https://www.academia.edu/11932385/_Re_Configuring_Security_Power_and_Privacy_Circumnavigating_Conceptual_Conundrums_through_Dissent_Anonymity_Software

Deek, Fadi P. and McHugh, James A. M. 2008. *Open Source: Technology and Policy*. New York : Cambridge University Press.

DeNardis, Laura. 2010. “The Privatization of the Internet Governance”. Yale Information Society Project Working Paper Draft. Paper presented at Fifth Annual GigaNet Symposium.

DeNardis, Laura. 2012. “Hidden Levers of Internet Control”. In *Information, Communication & Society*, 15:5, 720-738

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven-London : Yale University Press.

DeNardis, Laura, and Musiani, Francesca. 2016. “Governance by Infrastructure”. In *The Turn to Infrastructure in Internet Governance* edited by Francesca Musiani, Derrick. L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 3-21. Basingstoke-New York: Palgrave MacMillan

Danezis, George, Dingledine, Roger and Mathewson, Nicholas. 2003. “Mixminion: Design of a Type III Anonymous Remailer Protocol”. *In the Proceedings of the 2003 IEEE Symposium on Security and Privacy*, May 2003, 2-15. https://freehaven.net/anonbib/cache/minion-design.pdf

Dingledine, Roger. 2002. *The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven*. MIT M.Eng. Thesis. May 22, 2000. https://www.freehaven.net/doc/freehaven.ps

Dingledine, Roger. 2010. “Ten things to look for in a circumvention tool”. *In the Proceedings of China Rights Forum*, July 2010, 9p. http://svn.torproject.org/svn/projects/articles/circumvention-features.pdf

Dingledine, Roger, Mathewson, Nicholas and Syverson, Paul. 2004. “Tor: the Second Generation Onion Router”. *In the Proceedings of the 13th USENIX Security Symposium*, August 2004, 17p. https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

Dingledine, Roger, Mathewson, Nicholas and Syverson, Paul. 2005. *Challenges in deploying low-latency anonymity*. Tor Technical Report 2005-02-001 – NRL/CHACS Report 5540-625. https://www.nrl.navy.mil/itd/chacs/dingledine-challenges-deploying-low-latency-anonymity

Dingledine, Roger and Mathewson, Nicholas. 2006. “Anonymity Loves Company: Usability and the Network Effect”. *In the Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, UK, June 2006, 12p, http://freehaven.net/doc/wupss04/usability.pdf

Eco, Umberto. 2019. Postille a “Il nome della Rosa”. In *Il Nome della Rosa*, 663-702. Milano : Bompiani

Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of the Discourse in Cold War America*. Cambridge-London: The MIT Press

Edwards, Paul N. 1998. “Y2K: Millennial Reflections on Computers as Infrastructures”. In *History and Technology*, 15, 7-29

Edwards, Paul N. 2003. “Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems”. In *Modernity and Technology* edited by Brey, Philip, Misa, Thomas and Feenberg, Andrew, 185-226. Cambridge-London : The MIT Press

Edwards, Paul N. 2004. “‘A Vast Machine’: Standards as Social Technology”. In *Science Mag*, 304, 827-8.

Edwards, Paul N., Jackson, Steven J., Bowker, Geoffrey C. and Knoble, Cory P. 2007. *Understanding Infrastructure: Dynamics, Tensions, and Design. Lessons for New Scientific Cyberinfrastructures* https://deepblue.lib.umich.edu/handle/2027.42/49353

Eghbal, Nadia. 2016a. *Roads and Bridges. The Unseen Labour Behind Our Digital Infrastructure*. https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/

Eghbal, Nadia. 2016b. *The Lemonade Stand. A Handy Guide to Financial Support for Open Source*. https://github.com/nayafia/lemonade-stand

Fabernovel. 2014. *GAFAnomics: New Economy, New Rules*. Last Modified January 14, 2014. https://www.fabernovel.com/en/insights/economy/gafanomics-new-economy-new-rules-3

Federrath, Hannes, Hansen Marith and Waidner Micheal. 2011. “Andreas Pfitzmann 1958-2010: Pioneer of Technical Privacy Protection in the Information Society”. In *Privacy and Identity 2010, IFIP AICT 352*, edited by S. Fischer-Hübner et al. 349-52

Feenberg, Andrew. 1999. *Questioning Technology*. New York : Routledge.

Fisher, Mark. 2018. *Realismo Capitalista*. Translated by Valerio Mattioli. Roma : Nero.

Formenti, Carlo. 2006. “Libertà e rete: un’utopia americana?”. In *Rete. Dinamiche sociali ed innovazioni tecnologiche* edited by Ferraris, Pino, 47-60. Torino : Carrocci

Formenti, Carlo. 2008. *Cybersoviet. Utopie post-democratiche e nuovi media*. Milano : Raffaello Cortina

Formenti, Carlo. 2011. *Felici e Sfruttati*. Milano : Egea

Formenti, Carlo. 2012. *Informazioni di Parte – Intervento di Carlo Formenti*. Last Modified February 4, 2012. https://www.infoaut.org/clipboard/informazioni-di-parte-intervento-di-carlo-formenti

Galič, Masa, Timan, Tjerk and Koops, Bert-Jaap. 2017. “Bentham and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation”. In *Philosophy and Technology*, 30:1, 9-37

Gehl, Robert W. 2014. “Power/Freedom on the dark web: A digital ethnography of the Dark Web Social Network”, in *New Media and Society*, 18:7, 1219-35

Gehl, Robert W. 2018. *Weaving the Dark Web. Legitimacy on Freenet, Tor and I2P.* Cambridge-London : The MIT Press

Giannuli, Aldo. 2013. *Come i Servizi Segreti Usano i Media*. Milano : Ponte delle Grazie.

Gilmore, John. 1991. “Privacy, Technology and the Open Society”. Speech given at the first conference on Computers, Freedom and Privacy, March 28, 1991 https://www.toad.com/gnu.cfp.talk.txt

Goldshlag, David, Reed, Micheal and Syverson, Paul. 1997. *Privacy on the Internet*. Last Modified April 17, 1997 https://www.onion-router.net/Publications/INET-1997.html

Goldshlag, David, Reed, Micheal and Syverson, Paul. 1999. “Onion Routing for Anonymous and Private Internet Connections”. In *Communications of the ACM*, 42:2, February 1999, 5p. http://www.onion-router.net/Publications/CACM-1999.pdf

Goldsmith Jack. 2018. *The Failure of Internet Freedom*. Last Modified June 13, 2018. https://knightcolumbia.org/content/failure-internet-freedom

Goldsmith, Jack and Wu, Tim. 2006. *I Padroni di Internet. L'illusione di un mondo senza confini*. Translated by Bernardo Parrella. Milano : RGB

Greenwald, Glenn. 2014. *Sotto Controllo. Edward Snowden e la Sorveglianza di Massa*. Translated by Irene Annoni and Francesco Peri. Milano : Rizzoli.

Gülcü, Ceki and Tsudik, Gene. 1996. "Mixing E-mail with Babel". In the *Proceedings of the Network and Distributed Security Symposium – NDSS '96*, February 1996, 2-16.

Höne, Stefen. 2015. "The Birth of the Urban Passenger: Infrastructural Subjectivity and the Opening of the New York City Subway". In *City*, 19:2-3, 313-21

Invisible Committee. 2019. *Comitato Invisibile*. Translated by Marcello Tarì. Roma : Nero

Ippolita. 2005. *Open Non è Free. Comunità Digitali tra Etica Hacker e Mercato Globale*. Milano : Elèuthera editrice

Ippolita. 2007. *Il Lato Oscuro di Google. Passato e Futuro dell'Industria dei Metadati*. Milano : Feltrinelli

Ippolita. 2014. *La rete e' libera e democratica. Falso!*. Bari : Editori Laterza

Ippolita. 2017. *Tecnologie del Dominio. Lessico Minimo di Autodifesa Digitale*. Milano : Meltemi editore

Isenberg, David S. 1997. "The rise of the stupid network". In *Computer Telephony*, August 1997, 16-26

Jackson, Steven J., Edwards, Paul N., Bowker, Geoffrey C. and Knobel, Cory P. 2007. "Understanding Infrastructure: History, Heuristics and Cyberinfrastructure Policy". In *First Monday*, 12:6, https://www.firstmonday.org/ojs/index.php/fm/article/view/1904/1786

Khan, David. 1967. *The Codebreakers. The Story of Secret Writing*. London : Weidenfeld & Nicolson

Kempf, James and Austein, Rob. 2004. *The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture*. RFC 3724. https://tools.ietf.org/rfc/rfc3724.txt

Kelty, Christopher M. 2008. *Two Bits. The Cultural Significance of Free Software*. Durham : Duke University Press

Kelty, Christopher M. 2013. “There is no free software”. In *Journal of Peer Production*, 1:3, http://peerproduction.net/issues/issue-3-free-software-epistemics/debate/there-is-no-free-software/

Kleiner, Dimitri and Wyrick, Bryan. 2007. *Infoenclosure 2.0*. https://www.metamute.org/editorial/articles/infoenclosure-2.0

KRITIK. 2019. *Prontuario di sopravvivenza all’agonia del capitale*. Roma : DeriveApprodi

La Cecla, Franco. 2015. *Surrogati di Presenza. Media e Vita Quotidiana*. Bologna : Bébert Edizioni.

Levine, Yasha. 2017. *Surveillance Valley: The Secret Military History of the Internet*. New York : Public Affairs

Levy, Steven. 1994. *Hackers. Gli Eroi della Rivoluzione Informatica*. Translated by Ermanno Guarnieri and Luca Piercecchi. Milano : Shake Edizioni

Levy, Steven. 2002. *Crypto. I Ribelli del Codice in Difesa della Privacy*. Translated by Sergio Cicconi and Giancarlo Carlotti. Milano : Shake Edizioni.

Lewis, Sarah J. 2017. *Queer Privacy. Essays from the Margins of Society*. Mascherari Press

Lovink, Geert. 2008. *Zero Comments. Teoria Critica di Internet*. Translated by Alessandro Delfanti. Milano : Mondadori

Lovink, Geert. 2012. *Ossessioni Collettive. Critica dei social media*, Translated by Bernardo Parrella. Milano : Università Bocconi Editore

Lyon, David. 1997. *L’occhio elettronico. Privacy e Filosofia della Sorveglianza*. Translated by Giancarlo Carlotti. Milano : Feltrinelli

Lyon, David. 2002. *La società sorvegliata. Tecnologie di controllo della vita quotidiana*. Translated by Albino Zanin. Milano : Feltrinelli

Mathewson, Nicholas. 2002. *Verifying mostly-static information flow control in Java Bytecode*. MIT M.Eng. Thesis. May 22, 2000 http://www.wangafu.net/~nickm/thesis.ps

May, Timothy. 1994. *Crypto Anarchy and Virtual Communities*. https://nakamotoinstitute.org/virtual-communities/

Mazzucato, Mariana. 2018. *Lo Stato Innovatore*. Translated by Fabio Galimberti. Bari-Roma : Editori Laterza.

McLean, John D. and Heitmeyer, Constance. 1995. “High Assurance Computer Systems: a Research Agenda”. In *Proceedings of America in the Age of Information, National Science and Technology Council Committee on Information and Communications Forum*. February 23, 1995, 10p https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/McLeanHeitmeyer1995.pdf

McLuhan, Marshall. 2010. *Gli strumenti del comunicare*. Translated by Ettore Capriolo. Milano : Il Saggiatore

Medina, Eden. 2011. *Cybernetic Revolutionaries. Technology and Politics in Allende’s Chile*. Cambridge-London : The MIT Press

Milani, Carlo and Sasso, Savino. 2015. “Rete Oscura, Rete profonda, Reti Comunitarie. Risposte tattiche ai fenomeni di centralizzazione e censura”. In *Mondo Digitale*, 60:15, 22p

Morozov, Evgeny. 2011. *L'Ingenuità della Rete. Il Lato Oscuro della Libertà di Internet*. Translated by Marilena Renda and Fjodor Ardizzoia. Torino : Codice Edizioni

Musiani, Francesca. 2012. “Caring about the plumbing: On the Importance of Architecture in Social Studies of (Peer-to-Peer) Technology”. In *Journal of Peer Production*, 1, 8p.

Nafus, Dawn. 2011. “‘Patches do not have gender’: What is not open in open source sotware”. In *New Media and Society*, 14:4, 669-83

National Research Council. 2000. *Network-centric Naval Forces. A Transition Strategy for Enhancing Operational Capabilities*. Washington, DC : The National Academies Press

Naughton, John. 2000. *A Brief History of the Future. The Origins of the Internet*. London : Orion Books

Neumann, Laura J. and Star, Susan L. 1996. “Making Infrastructure: The Dream of a Common Language”. In *Proceedings of the Participatory Design Conference* (PDC ‘96), 231-240

Nhan, Johnny and Carroll, Bruce A. 2012. “The Offline Defense of the Internet: An Examination of the Electronic Frontier Foundation”. In SMU Science and Technology Law Review, 15, 389-401

Nissenbaum, Helene. 2009. *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford : Stanford University Press

Nordenstreng, Kaarle and Schiller, Herbert. 1979. *National Sovereignty and International Communication: A Reader*. Nordwood : Ablex

Nye, J.S. 2005. *Soft power. Un nuovo futuro per l'America*. Translated by Stefano Suigo. Torino : Einaudi.

Papadopoulous, Dimitris. 2018. *Experimental Practice. Technoscience, Alterontologies, and More-Than-Social Movements*. Durham-London : Duke University Press

Pappacharrisi, Zizi A. 2010. *A Private Sphere: Democracy in a Digital Age*. Cambridge : Polity Press

Parisier, Eli. 2012. *Il filtro. Quello che Internet ci nasconde*. Translated by Bruna Tortorella. Milano : Il Saggiatore

Pfitzmann, Andreas, Pfitzmann, Brigit and Waidner, Michael. 1991. “ISDN-mixes: Untraceable communication with very small bandwidth”. In the *Proceedings of the GI/ITG Conference on Communication in Distributed Systems*, February 1991, 451-63

Philips, Charles E., Demurjian, Steven A., Ting, T.C. 2002. “Information Sharing and Security in Dynamic Coalitions”. In *SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*, June 2002, 87-96

Philo, Greg. 1990. *Seeing is believing. The Influence of Television.* London : Routledge.

Postel, Jon (ed). 1980. *DoD Standard Internet Protocol*. RFC 760. https://tools.ietf.org/rfc/rfc760.txt

Postel, Jon (ed). 1981. *Internet Protocol*. RFC 791. https://tools.ietf.org/rfc/rfc791.txt

Powell, Alexander. 1919. *The Army Behind the Army*. New York : Charles Scribner's Sons.

Powers, Shawn M. and Jablonksi, Micheal. 2015. *The Real Cyber War. The Political Economy of Internet Freedom*. Champaign : The University of Illinois Press

Raymond, Eric S. 2000a. *The Cathedral and the Bazaar*. http://www.catb.org/esr/writings/cathedral-bazaar/cathedral-bazaar/

Raymond, Eric S. 2000b. *Homesteading the Noosphere*. http://www.catb.org/esr/writings/homesteading/homesteading/

Richterich, Annika. 2018. *The Big Data Agenda: Data Ethics and Critical Data Studies*. London : University of Westminster Press

Rodotà Stefano. 2004. *Tecnopolitica. La Democrazia e le Nuove Tecnologie della Comunicazione.* Roma-Bari : Editori Laterza

Saco, Diana. 1999. "Colonizing Cyberspace: National Security and the Internet". In *Cultures of Insecurity: States, Communities, and the Production of Danger*, edited by Weldes, Jutta, Laffey, Mark, Gusterson, Hugh and Duvall, Raymond, 293-318. Minneapolis-London : University of Minnesota Press

Sandvig, Christian. 2013. "The Internet as Infrastructure". In *The Oxford Handbook of Internet* Studies, edited by Dutton, William H., 86-106. Oxford : Oxford University Press

Sargsyan, Tatevik. 2016. "The Turn to Infrastructure in Privacy Governance". In *The Turn to Infrastructure in Internet Governance* edited by Francesca Musiani, Derrick. L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 189-201. Basingstoke-New York: Palgrave MacMillan

Sassen, Saskia. 2008. *Una Sociologia della Globalizzazione*. Translated by Piero Arlorio. Torino : Einaudi

Sassen, Saskia, 2008b. *Territorio, autorità, diritti. Assemblaggi dal Medioevo all'età globale*. Translated by Nuccia Malinverni and Giuseppe Barile. Milano : Mondadori.

Schneier, Bruce. 2015. *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World.* New York-London : W.W. Norton & Company.

Shirky, Clay. 2010. *Cognitive Surplus: Creativity and Generosity in a Connected Age*. London : Allen Lane.

Shultz, George P. 1985. “New Realities and New Ways of Thinking”. In *Foreign Affairs*, 63:4, 705-721

Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge-London : Harvard University Press

Sordi, Paolo and Fioramonte, Domenico. 2019. “Geopolitica della Conoscenza Digitale. Dal Web Aperto all’Impero di GAFAM”. In *DigitCult. Scientific Journal on Digital Cultures*, 4:1, 21-36

Snowden, Edward. 2019. *Errore di sistema*. Translated by Netphilo Publishing. Longanesi : Milano.

Sparti, Davide. 2015. “L’infanzia Presa sul Serio. Dalla Metafisica alla Presenza alla Presenza come Trama Relazionale”. In *Surrogati di presenza. Media e Vita Quotidiana*, edited by Franco La Cecla, 152-68. Bologna: Bébert Edizioni

Stalder, Felix. 2010. *Autonomy and Control in the Era of Post-Privacy*. http://felix.openflows.com/node/143

Staltz, André. 2019. *Software Below the Poverty Line*. https://staltz.com/software-below-the-poverty-line.html

Star, Susan L. 1999. “The Ethnography of Infrastructure”. In *American Behavioral Scientist*, 43:3, 377-91

Star, Susan L. 2002. “Infrastructure and ethnographic practice”. In *Scandinavian Journal of Information System*, 14:2, 107-22

Star, Susan L. and Ruhleder, Karen. 1996. “Steps Towards an Ecology of Infrastructure: Design and Access for Large Information Spaces”. In *Information System Research*, 7:1, 111-34

Suchman, Lucy, Trigg, Randall and Blomberg, Jeanette. 2002. “Working artefacts: ethnomethods of the prototype”. In *British Journal of Sociology*, 53:2, 163-79

Sundblad, Yngve. 2011. “UTOPIA: Participatory Design from Scandinavia to the World”. In *History of Nordic Computing 3. HiNC 2010. IFIP Advances in Information and Communication Technology*, vol 350.

Tapscott, Don and Williams, Anthony D. 2008. *Wikinomics 2.0*. Milano : Rizzoli.

Tenner, Edward. 2001. *Perché le cose si ribellano*. Translated by Nicoletta Santambrogio. Milano : Rizzoli

Terranova, Tiziana. 2000. “Free Labor: Producing Culter for the Digital Economy”. In *Social Text*, 63:2, 33-58

Tomlinson, John. 1999. *Globalization and Culture*. Cambridge : Polity.

Vaidhyanathan, Siva. 2012. *The Googlization of Everything (and why we should worry)*. Oakland : University of California Press.

Vecchi, Benedetto. 2015. *La Rete dall’Utopia al Mercato*. Roma : Manifestolibri

Virilio, Paul. 1994. *Bunker Archaeology*. Translated by George Collins. New York : Princeton Architectural Press.

Vischer, Robert, Fiedler, Conrad, Göller, Adolf, Wölfflin, Heinrich, Schmarsow, August and Hildebrand, Adolf. 1993. *Empathy, Form, and Space: Problems in German Aesthetics, 1873-1893*. Translated by Harry Francis Mallgrave, Eleftherios Ikonomou, Heinrich Wölfflin. Santa Monica : Getty Center for the History of Art and the Humanities

Weber, Rolf. H. 2012. “How Does Privacy Change in the Age of Internet?. In *Internet and Surveillance. The Challenges of Web 2.0 and Social media*, edited by Fuchs, Cristian, Boersma, Kees, Albrechtslund, Anders and Sandoval, Marisol, 273-94. New York-London : Routledge

Weber, Steven. 2004. *The Success of Open Source*. Cambridge : Harvard University Press

Williams, Sam. 2003. *Codice Libero. Richard Stallman e la Crociata per il Software Libero*. Milano : Apogeo.

Winner, Langdon. 1986. *The Whale and the Reactor. A Search for Limits in an Age of High Technology*. Chicago-London : The University of Chicago Press

Zhu. Henry. 2019. *Open Source: Charity or Business*. https://github.com/hzoo/open-source-charity-or-business/

Zielinksky, Siegfried and Custance, Gloria. 2006. *Deep Time of the Media*. Cambridge-London : The MIT Press.

Zuboff, Shoshana. 2019a. *Il Capitalismo di Sorveglianza. Il Futuro dell'Umanità nell'Era dei Nuovi Poteri*. Translated by Paolo Bassotti. Roma : Luiss University Press

Zuboff, Shoshana. 2019b. "Surveillance Capitalism and the Challenge of Collective Action". In *New Labor Forum*, 28:1, 10-29.

Notes

1. Approaching Tor through history and theory

[1] In the P2P model there is no functional distinction between users, and anyone taking part in the network acts either as recipient and sender

[2] Porter, John. 2019. “German state bans Office 365 in schools, citing privacy concerns”. *The Verge*, July 15, 2019. https://www.theverge.com/2019/7/15/20694797/hesse-german-state-gdpr-office-365-schools-illegal-data-protection

[3] McFadden, Cynthia. 2016. “Putin Wants to Push Microsoft Out of Russia in Battle with U.S.”. *NBC News*, November 1, 2016. https://www.nbcnews.com/news/us-news/putin-wants-push-microsoft-out-russia-battle-us-n674781

[4] Pizio, Daniele. 2014. “Fughe digitali dal controllo”. *Il manifesto*, May 9, 2014. https://ilmanifesto.it/fughe-digitali-dal-controllo/

[5] Martin, Alexander. 2019. “China 'bans foreign computer equipment and software from state offices'”. *Sky News*, December 9, 2019. https://news.sky.com/story/china-bans-foreign-computer-equipment-and-software-from-state-offices-11882174

[6] Jancer, Matt. 2015. “Brazil builds undersea internet cable to protect online privacy”. *Wired UK*, April 2, 2015. https://www.wired.co.uk/article/brazilian-sea-spanner

[7] Matsakis, Louise. 2019. “Apple's Good Intentions Often Stop at China's Borders”. *Wired*, October 17, 2019. https://www.wired.com/story/apple-china-censorship-apps-flag/

[8] The Tor Project has developed Tor Metrics a database that “archives historical data about the Tor ecosystem, collects data from the public Tor network and related services, and assists in developing novel approaches to safe, privacy preserving data collection”. Tor Metrics is the primary source of the statistical data about the Tor network that I will present in this thesis. For more information about Tor Metrics philosophy and design see: Tor Metrics. “About Tor Metrics” https://metrics.torproject.org/about.html Last accessed February 7, 2020

[9] Tor Metrics. “Users”. Accessed February 7, 2020. https://metrics.torproject.org/userstats-relay-country.html

[10] Tor Metrics. “Servers”. Accessed February 7, 2020. https://metrics.torproject.org/networksize.html

[11] Tor Metrics. “Traffic”. Last accessed February 7, 2020. https://metrics.torproject.org/bandwidth.html

[12] Tor Metrics. “Onion Services”. Accessed February 7, 2020. https://metrics.torproject.org/hidserv-rend-relayed-cells.html

[13] Tor Metrics. “Traffic (08/19/2010 – 08/19/2020)”. Accessed August 19, 2020. https://metrics.torproject.org/bandwidth.html?start=2010-08-19&end=2020-08-19

[14] Tor Metrics. “Onion Services (08/20/2010 – 09/19/2020)”. Accessed August 19, 2020. https://metrics.torproject.org/hidserv-rend-relayed-cells.html?start=2010-08-20&end=2020-08-19

[15] In order to have a general idea about the size of the Tor Ecosystem see: Tor Project. “Projects Overview”. Accessed August 19, 2020. https://2019.www.torproject.org/projects/projects.html.en and, Tor Project. “Community Project Overview”. Accessed August 19, 2020. https://2019.www.torproject.org/projects/community.html.en and, Tor Project. “The Tor Ecosystem”. Accessed August 19, 2020. https://svn-archive.torproject.org/svn/projects/presentations/2013-11-t3am-tor-ecosystem.pdf. Yet, the amount of Tor-based software is actually much bigger: indeed, a simple research on GitHub reveals that on the platform there are 870 repositories labeled under the tag #tor

[16] Tor Blog. 2011. “Recent events in Egypt”. Last modified January 29, 2011. https://blog.torproject.org/recent-events-egypt

[17] Tor Metrics. “Number of directly connecting clients in Turkey from 03/01/2014 to 04/30/2014”. Accessed February 7, 2020. https://metrics.torproject.org/userstats-relay-country.html?start=2014-03-01&end=2014-04-30&country=tr&events=on

[18] Tor Metrics. “Number of directly connecting clients in Lybia from 10/09/2010 to 01/07/2014”. Accessed February 7, 2020. https://metrics.torproject.org/userstats-relay-country.html?start=2010-10-09&end=2014-01-07&country=ly&events=on

[19] Such as Globaleaks (https://www.globaleaks.org) and SecureDrop (https://www.securedrop.org/)

[20] Facebook. 2014. “Making Connections to Facebook more Secure”. Last modified October 31, 2014. https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237

[21] Facebook. 2018. “Making connections to Facebook over Tor faster”. Last modified November 20, 2018. https://www.facebook.com/notes/facebook-over-tor/making-connections-to-facebook-over-tor-faster/1729157350524311/

[22] The Cloudflare Blog. 2018. “Introducing the Cloudflare Onion Service”. Last modified September 20, 2018. https://blog.cloudflare.com/cloudflare-onion-service/

[23] The Cloudflare Blog. 2018. “Introducing DNS Resolver for Tor”. Last modified June 5, 2018. https://blog.cloudflare.com/welcome-hidden-resolver/

[24] Tor Blog. 2014. “Partnering with Mozilla”. Last modified November 11, 2014. https://blog.torproject.org/partnering-mozilla

[25] Mozilla Wiki. “Tor Uplift”. Accessed February 7, 2020. https://wiki.mozilla.org/Security/Tor_Uplift

[26] Mozilla. "Mozilla Research Grants 2019H1". Accessed February 7, 2020. https://mozilla-research.forms.fm/mozilla-research-grants-2019h1/forms/6510

[27] BBC News. 2019. "BBC news launches 'dark web' Tor mirror". *BBC News*, October 23, 2019. https://www.bbc.com/news/technology-50150981

[28] Sandvik, Runa. 2017. "The New York Times is Now Available as a Tor Onion Service". *The New York Times*, October 27, 2017. https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482?gi=12a035863fd3

[29] Jumpelt, Cristoph. 2019. "Deutche Welle websites accessible via Tor-Protocol". *Deutsche Welle*, May 7, 2019. https://www.dw.com/en/deutsche-welle-websites-accessible-via-tor-protocol/a-51338328

[30] Central Intelligence Agency. 2019. "CIA's Latest Layer: An Onion Site". Last modified May 7, 2019. https://www.cia.gov/news-information/featured-story-archive/2019-featured-story-archive/latest-layer-an-onion-site.html

[31] Pornhub. 2020. "Pornhub Launches Tor Mirror Site to Bolster User Privacy and Ensure Platform Security". Last modified January 22, 2020. https://www.pornhub.com/press/show?id=1911

[32] "Request for Comments" or RFC are documents covering "many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions, and sometimes humor". Published by the IETF, they describe Internet protocols, specifications, standards and working procedures. See: IETF. "RFC". Accessed June 1, 2020. https://ietf.org/standards/rfcs/

[33] RFC 791 replaces RFC 760, which in turn replaces IEN 26 and IEN 28. IEN stands for "Internet Experiment Note": these are a series of sequentially numbered reports pertinent to the early development of the Internet and published in parallel to RFCs. Both IEN 26 and IEN 28 were published on February 1978. See: IETF. "Internet Experiment Note Index". Accessed June 1, 2020. https://www.ietf.org/rfc/ien/ien-index.html

[34] Clark (1988, 103) explains this hierarchy of priorities in this way: "During wartime, one is less concerned with detailed accounting of resources used than with mustering whatever resources are available and rapidly deploying them in an operational manner. While the architects of the Internet were mindful in accountability, the problem received very little attention during the early stages of the design, and is only now being considered. An architecture primarily for commercial development would clearly place these goals at the opposite end of the list".

[35] The Time to Live (or TTL) is the maximum time the datagram is allowed to remain in the Internet system.

[36] The Type of Service (or ToS) provides an indication of the abstract parameters of the quality of service desired

[37] Fun comes from the sentence reported by the last player being often very different from the starting one, also due to the combination and addition of successive errors of interpretation. However this is

not relevant to our analogy, nor to this thesis since this kind of errors on the Internet are usually managed by the TCP and not the IP.

[38] It is worth noting that the production of intelligence is just one of the aims of T/A. Along with surveillance, T/A can be used in order to deceive an enemy. With the Operation Quicksilver, which preceded the D-Day, the Allies convinced the Nazis that their target was Pas-De-Calais (instead of Normandy). In order to do that, the Allies established fake communication networks which activity would appear to support the preparations for a major invasion of Calais. See Borrmann et al 2013, 36-7

[39] Laporte, Leo. 2015. "Triangulation 229: Paul Syverson, Inventor of Tor". Last modified December 15, 2015. https://www.youtube.com/watch?v=_1xbCNyJVzU

[40] Laporte. Leo. 2015. "Triangulation 148: Vinton Cerf Part II". Last modified April 21, 2014. https://www.youtube.com/watch?v=L-N4lQnHwyU

[41] U.S Naval Research Laboratory. "2019 NRL Factbook". Accessed May 09, 2020. https://www.nrl.navy.mil/content_images/2019_FactBook.pdf

[42] U.S. Naval Research Laboratory. "ITD Home". Accessed February 17, 2020. https://www.nrl.navy.mil/itd/

[43] U.S. Naval Research Laboratory. "Center for High Assurance Computer Systems". Accessed February 17, 2020. https://www.nrl.navy.mil/itd/chacs/

[44] U.S. Naval Research Laboratory. "CHACS' Formal Methods Section". Accessed February 17, 2020. https://www.nrl.navy.mil/itd/chacs/5543

[45] Onion Routing. "History". Accessed May 10, 2020. https://www.onion-router.net/History.html

[46] DARPA. "DARPA seeks research into next generation information systems". Accessed May 10, 2020. https://www.govcon.com/doc/darpa-seeks-research-into-next-generation-inf-0001

[47] Statement by Tony Tether Submitted to the Committee on Science US House of Representatives. May 14, 2003. https://www.darpa.mil/attachments/TestimonyArchived(May%2014%202003).pdf

[48] This information is elicited by the above mentioned Onion Routing history web page

[49] DARPA. "Onion Routing: Anonymous Communications Infrastructures". Accessed May 10, 2020. https://web.archive.org/web/19990203140616/http://www.darpa.mil/ito/Summaries97/E922_0.html

[50] Reed, MIcheal. 2011. "[tor-talk] Iran cracks down on web dissident technology". *Tor-talk mailing list*, March 22, 2011. https://lists.torproject.org/pipermail/tor-talk/2011-March/019913.html

[51] Onion Routing. "Making Anonymous Communication". Slides by Paul Syverson, June 8, 2004. https://www.onion-router.net/Publications/Briefing-2004.pdf Accessed May 10,2020

[52] Free Haven. "Anonymity Bibliography". Accessed May 10, 2020. https://www.freehaven.net/anonbib/full/date.html

[53] Syverson, Paul. 2011. "[tor-talk] Iran cracks down on web dissident technology". *Tor-talk mailing list*, March 21, 2011. https://lists.torproject.org/pipermail/tor-talk/2011-March/019868.html

[54] Paul Syverson’s Google Scholar Page https://scholar.google.com/citations?hl=en&user=QDnC2nAAAAAJ&oi=sra

[55] Laporte, Leo. 2015. “Triangulation 229: Paul Syverson, Inventor of Tor”. Last modified December 15, 2015. https://www.youtube.com/watch?v=_1xbCNyJVzU

[56] Java Information Flow. “Homepage”. Accessed May 10, 2020. http://www.cs.cornell.edu/jif/

[57] Mathewson, Nick. 2014. “6.858 Fall 2014 Lecture 19: Tor”. Last modified November 19, 2014 https://www.youtube.com/watch?v=rIf_VZQr-dw Unless otherwise stated, in this paragraph all the quotations attributed to Mathewson are extrapolated from this footage.

[58] Not only in the academic field. The British GCHQ, in some of the documents seized by Edward Snowden from the NSA databases, defines Tor as "the king of high-secure, low-latency anonymity systems. Currently there are no contenders to the throne in waiting”

[59] On the other hand, this is precisely the premise opening 1981 Chaum's paper about Mix Net – a document being universally considered as the seminal work in the context of anonymous digital communication networks.

[60] Live Science. 2014. “How to surf the web without leaving a trace”. Last modified March 18, 2014. https://www.youtube.com/watch?v=3fyy7UPrV94

[61] Kreiser, John. 2006. “Cracking the Great Firewall of China”. *CBS News*, February 15, 2006. https://www.cbsnews.com/news/cracking-the-great-firewall-of-china/

[62] Talbot, David. 2009. “Dissent Made Safer”. *The MIT Technology Review*, April 21 2009. https://www.technologyreview.com/s/413091/dissent-made-safer/

[63] Netzpolitik. 2012. “NetzpolitikTV: Roger Dingledine about the TOR-Project”. Last modified May 22, 2012. https://www.youtube.com/watch?v=itMZ0Qq-rGk

[64] Wittmeyer, Alicia P.Q. 2012. “The FP Top 100 Global Thinkers”. *Foreign Policy*, November 26, 2012. https://foreignpolicy.com/2012/11/26/the-fp-top-100-global-thinkers-2/

[65] There are also other relevant ones that will be discussed later on in chapter 5, like Tor’s public perception, the imaginaries it fuels and the sustainability of the infrastructure.

[66] See Chapter 5 on the role of the perception of Tor and its influence on the effectiveness of the network.

[67] Talbot, David. 2009. “Dissent Made Safer”. *The MIT Technology Review*, April 21, 2009. https://www.technologyreview.com/s/413091/dissent-made-safer/

[68] For instance, a network like PipeNet provides strong anonymity but its design allows a single user to shutdown the entire infrastructure since it lacks a traffic congestion system. Crowds does not use encryption, “so any node on a circuit can read users’ traffic” and manipulate it. Herbivore or P5 “are designed primarily for communicating among peers” and are closed network, obviously not suitable for surfing the web.

[69] Moreover, the Tor version released in 2004 presents the implementation of new features aimed at addressing several limitations affecting the onion routing prototype created by Syverson, Reed and Goldshlag in 1996.

[70] For instance HTTP and HTTPS (for Internet browsing), POP3, IMAP and SMTP (for email), XMPP and IRC (for chat and instant messaging) are just a few among the most relevant.

[71] A detailed technical explanation of Tor is out of the scope of this thesis. For a good starting point on the topic see: Tor Project. "Support". Accessed February 23, 2020. https://support.torproject.org/ and, Skerritt, Brandon. 2019. "How does Tor really work? The definitive visual guide". Last modified June 19, 2019. https://skerritt.blog/how-does-tor-really-work

[72] Indeed, the onion routing prototype was based on "a single multiply encrypted data structure" (Dingledine et al 2004, 1)

[73] Such features (traffic integrity check and network congestion protocol) originally were not implemented in the Tor protocol v0 released in 1996.

[74] DEFCONConference. 2013. "DEF CON 21 – Runa A Sandvik – Safety of the Tor network". Last modified December 23, 2013. https://www.youtube.com/watch?v=qWr5D2RoXoo

[75] Feroz, Anas. 2018. "War on privacy, Tor and the Forgotten Hero: An Interview with Shava Nerad". *Online Privacy Tips*, June 15, 2018. https://www.onlineprivacytips.co/interview/shava-nerad-interview/

[76] EFF. 2004. "EFF joins Forces with Tor Software Project". Last modified December 21, 2004. https://www.eff.org/press/archives/2004/12/21-0

2. Methodological approach to infrastructure

[1] Tor Project. "lists.torproject.org Mailing Lists". Accessed August 26, 2020. https://lists.torproject.org/cgi-bin/mailman/listinfo

[2] Tor Project. "Tor Bug Tracker and Wiki". Accessed August 26, 2020. http://trac.torproject.org/

[3] Tor Project. "Available Reports. Tor Bug Tracker and Wiki". Accessed August 26, 2020. http://trac.torproject.org/projects/tor/report

[4] Tor Project. "Tor's source code". Accessed August 26, 2020. https://gitweb.torproject.org/tor.git

[5] Internet Archive. "The Way Back Machine". Accessed August 26, 2020. https://archive.org/web/web.php

[6] Tor Project. "Reports". Accessed August 26, 2020. https://www.torproject.org/about/reports/

[7] Tor Project. "Tor Blog". Accessed August 26, 2020. https://blog.torproject.org/

[8] Tor Projects. "Metrics". Accessed August 26, 2020. https://metrics.torproject.org/

[9] According to the Tor wiki, the Tor Network team is "a group of Tor people who are working on Tor back-end: the program called Tor, the pluggable transports, the bridge distribution, the network

simulators, the scripts that supports directory authorities, onion services" https://trac.torproject.org/projects/tor/wiki/org/teams/NetworkTeam

[10] Tor Project. "About. Tor Metrics". Accessed August 26, 2020. https://metrics.torproject.org/about.html

[11] Qubes OS. "Homepage". Accessed August 26, 2020. https://www.qubes-os.org

[12] University of Leicester. "Research Code of Conduct and Ethics". Accessed August 26, 2020. https://www2.le.ac.uk/offices/researchsupport/policyandstrategy/research-code-of-conduct-and-ethics-1

[13] Signal. "Home". Accessed August 26, 2020. https://signal.org/

3. The Tor's funding system

[1] According to the GNU manifesto "a program is free software if the program's users have the four essential freedoms: the freedom to run the program as you wish, for any purpose (freedom 0). The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this. The freedom to redistribute copies so you can help others (freedom 2). The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this". See: GNU Project. "What is free software?" Accessed September 20, 2020. https://www.gnu.org/philosophy/free-sw.html

[2] The Tor Project. "Tor Project | Reports". Accessed May 27, 2020. https://www.torproject.org/about/reports/

[3] Open Tech Fund. "OTF | Annual Reports". Accessed August 27, 2020. https://www.opentech.fund/results/annual-reports/

[4] However, due to the COVID-19 pandemic, the staff has been cut by a third. See: Tor Blog. 2020. "COVID-19's impact on Tor". Last modified April 17, 2020. https://blog.torproject.org/covid19-impact-tor

[5] Actually, according Privcount (https://github.com/privcount/privcount), a new research tools for privacy-preserving statistics developed by the Tor Project, the number of daily users of the network is higher than this. The new estimation is between 2.5 and 8 million. For more information see: Tor Blog. 2019. "A better Internet is possible. I've seen it". Last modified November 4, 2019. https://blog.torproject.org/better-internet-possible-ive-seen-it

[6] Last time I witnessed a public discussion about Tor Project financial organization was in December 2017 in Leipzig (Germany), when Roger Dingledine, founder and leader of the project, kept a Tor Q&A session at the 34th edition of the hacker meeting Chaos Communication Congress (#34C3). In this paragraph I make several references to this talk.

[7] General Service Administration. “CFDA 47.070”. Accessed May 29, 2020. https://beta.sam.gov/fal/cef187eb416e4990b2943fc201f684a7/view?keywords=CFDA%2047.070&sort=-relevance&index=&is_active=true&page=1

[8] National Science Foundation. “Computer and Information Science and Engineering (CISE) Active Awards”. Accessed May 29, 2020. https://www.nsf.gov/awards/award_visualization.jsp?org=CISE

[9] Standford Research International. “SRI Fact sheet (2013) ”. Accessed May 29, 2020. https://www.sri.com/sites/default/files/brochures/sri-fact-sheet.pdf

[10] The remainder of the money provided by the DoD through SRI, goes under the name “SRI Lights”. It has been provided in 2014 and 2015. However, there is no CFDA number associated with SRI Lights contracts and I have not been able to find any relevant information about them.

[11] General Service Administration. “CFDA 12.335”. Accessed May 29, 2020. https://beta.sam.gov/fal/c948c347a293a3b15e39251efd522f99/view?keywords=CFDA%2012.335&sort=-relevance&index=&is_active=true&page=1

[12] Space And Naval Warfare Systems Center. “About”. Accessed May 29, 2020. http://www.public.navy.mil/spawar/Pages/Organization.aspx

[13] General Service Administration. “CFDA 19.345”. Accessed May 29, 2020. https://beta.sam.gov/fal/8d45b54d9892478fa7def8b1c705a924/view?keywords=CFDA%2019.345&sort=-relevance&index=&is_active=true&page=1

[14] U.S. Department of State. “Bureau of Democracy, Human Rights and Labor”. Accessed May 29, 2020. https://www.state.gov/bureaus-offices/under-secretary-for-civilian-security-democracy-and-human-rights/bureau-of-democracy-human-rights-and-labor/

[15] Along with the IPDRL, DRL manages another important fund, that is the Human Rights and Democracy Fund (HRDF). Established by the US congress in 1998, HRDF is defined as “a ‘venture capital fund’ for democracy and human rights”.

[16] Usaspending.gov. “CFDA 19.345”. Accessed May 29, 2020. https://www.usaspending.gov/#/search/accd5024c33954ddd4237cafa2b966ee

[17] More precisely 1.998.959.419 $.

[18] Tor Project. “Sponsors”. Accessed May 29, 2020. https://www.torproject.org/about/sponsors/

[19] This calculation also includes the funds donated to Tor by Internews Europe ($ 275,940) and SRI Lights ($ 878,016), without which the situation does not change much ($ 7,960,453, corresponding to 49.55% of the Tor budget).

[20] Tor's 990 modules from the years 2016 and 2017 were only released after this chapter was written, which is why I only marginally drew on them. They mark the emergence of some new trends in Tor's funding system (like a specific weight of donations from private companies) which I will briefly explore in chapter 5. However, the reading of the data contained therein confirms the salient points of the analysis that have emerged so far.

[21] OTF. “Annual Reports”. Accessed Jun 9, 2020. https://www.opentech.fund/results/annual-reports/

[22] OTF. “Supporting Internet Freedom Worldwide”. Accessed June 9, 2020. https://www.opentech.fund/

[23] OTF. “Values and Principles”. Accessed June 9, 2020. https://www.opentech.fund/about/values-principles/

[24] OTF. “2015 Annual Report”. Accessed June 9, 2020. https://public.opentech.fund/documents/2015otfannualreport.pdf

[25] OTF. “2012 Annual Report”. Accessed June 9, 2020. https://www.opentech.fund/documents/4/otf_2012_annual_report_final_public.pdf

[26] OTF. “2013 Annual Report”. Accessed June 9, 2020. https://www.opentech.fund/documents/5/otf2013annualreportfinal.pdf

[27] OTF. “2014 Annual Report”. Accessed June 9, 2020. https://www.opentech.fund/documents/6/2015otfannualreport.pdf

[28] OTF. “Tor Project”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/tor-project/

[29] OTF. “Preparing Tor Browser For Android For Mainstream Adoption”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/preparing-tor-browser-android-mainstream-adoption/

[30] OTF. “Tor Onion Services”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/tor-onion-services/

[31] OTF. “Tor Bridge Distribution”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/tor-bridge-distribution/

[32] OTF. “Tor Metrics”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/tor-metrics/

[33] OTF. “OONI: Open Observatory of Network Interference”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/ooni-open-observatory-of-network-interference/

[34] OONI. “Open Observatory of Network Intereference”. Accessed June 10, 2020. https://ooni.org/

[35] OTF. “Tails”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/tails/

[36] Tails. “Tails”. Accessed June 10, 2020. https://tails.boum.org

[37] Globaleaks. “The Open Source Whistleblowing Software”. Accessed June 10, 2020. https://www.globaleaks.org/

[38] OTF. “Globaleaks”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/globaleaks/

[39] NoScript. “JavaScript/Java/Flash blocker for a safer Firefox experience”. Accessed June 10, 2020. https://noscript.net/

[40] OTF. “NoScript”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/noscript/

[41] Briar. “Secure Messaging, Anywhere”. Accessed June 10, 2020. https://briarproject.org/

[42] OTF. “Briar”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/briar/

[43] Cupcake Bridge. “Create new pathways into Tor”. Accessed June 10, 2020. https://github.com//glamrock/cupcake

[44] OTF. “Cupcake Bridge”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/cupcake-bridge/

[45] OTF. “The Tor BSD Diversity Project”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/tor-bsd-diversity-project/

[46] The Tor BSD Diversity Project. “About”. Accessed June 10, 2020. https://torbsd.org/about.html

[47] OTF. “Derechos Digitales”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/derecho-digitales/

[48] Onion Browser. “About”. Accessed June 10, 2020. https://onionbrowser.com/about

[49] OTF. “Onions on Apples”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/onions-apples/

[50] Tor Blog. 2017. “We’ll Pay You to #HackTor”. Last modified July 20, 2017. https://blog.torproject.org/blog/we-will-pay-you-to-hack-tor-bug-bounty

[51] Tor Blog. 2018. “We launched a Live Brand Styleguide”. Last modified March 6, 2018. https://blog.torproject.org/we-launched-live-brand-styleguide

[52] OONI. 2017. “OONI partner gathering”. Last modified July 24, 2017. https://ooni.org/post/ooni-partner-gathering-2017/

[53] OTF. “Internet Freedom Festival”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/internet-freedom-festival/

[54] Internet Freedom Festival. “Homepage (Snapshot 23/12/18/)”. Accessed June 10, 2020. https://web.archive.org/web/20181223053531/https://internetfreedomfestival.org/

[55] Qubes OS. “A reasonably secure operative system”. Accessed June 10, 2020. https://www.qubes-os.org/

[56] OTF. “Qubes OS”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/qubes-os/

[57] Subgraph Os. “About Us”. Accessed June 10, 2020. https://subgraph.com/about-us/index.en.html

[58] OTF. “Subgraph OS”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/subgraph-os/

[59] Leap. “Home”. Accessed June 10, 2020. https://leap.se/

[60] OTF. “Leap Encryption Access project”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/leap-encryption-access-project/

[61] WireGuard. “Wireguard: fast, modern, secure VPN tunnel”. Accessed June 10, 2020. https://www.wireguard.com/

[62] OTF. “WireGuard”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/wireguard/

[63] Mailvelope. “About”. Accessed June 10, 2020. https://mailvelope.com/en/about

[64] OTF. “Mailveope”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/mailvelope/

[65] Lantern. “Open Internet For All”. Accessed June 10, 2020. https://lantern.io/en_US/index.html

[66] OTF. “Lantern”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/lantern/

[67] OTF. “Cryptocat”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/cryptocat/

[68] Certbot. “About”. Accessed June 10, 2020. https://certbot.eff.org/

[69] OTF. “Certbot improvements”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/certbot-improvements/

[70] OTF. “DNSPrivacy”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/dnsprivacy/

[71] Signal. “Home”. Accessed June 10, 2020. https://signal.org/

[72] OTF. “Open Whisper System”. Accessed June 10, 2020. https://www.opentech.fund/results/supported-projects/open-whisper-systems/

[73] Signal Blog. 2016. “WhatsApp's Signal Protocol integration is now complete”. Last modified April 5, 2016. https://signal.org/blog/whatsapp-complete/

[74] Signal Blog. 2016. “Facebook Messenger deploys Signal Protocol for end-to-end encryption”. Last modified July 8, 2016. https://signal.org/blog/facebook-messenger/

[75] Signal Blog. 2016. “Open Whisper Systems partners with Google on end-to-end encryption for Allo”. Last modified May 18, 2016. https://signal.org/blog/allo/

[76] Signal Blog. 2018. “Signal Partners With Microsoft to bring end-to-end encryption to Skype”. Last modified January 11, 2018. https://signal.org/blog/skype-partnership/

[77] Nextcloud Blog. 2018. “Nextcloud 14 now available with Video Verification, Signal/Telegram 2FA support, Improved Collaboration and GDPR compliance”. Last modified September 10, 2018. https://nextcloud.com/blog/nextcloud-14-now-available-with-video-verification-signaltelegram-2fa-support-improved-collaboration-and-gdpr-compliance/

[78] Signal Blog. 2018. “Signal Foudation”. Last modified February 21, 2018. https://signal.org/blog/signal-foundation/

[79] Covert, Adrian. 2014. “Facebook buys WhatsApp for $19 billion”. CNN Business, February 19, 2014. https://money.cnn.com/2014/02/19/technology/social/facebook-whatsapp/index.html

[80] The site https://torpat.ch/ provides an updated list of the patches backported from TBB to Firefox. The site is maintained by Arthur Edelstein, TBB lead developer.

[81] OTF. “Preparing Tor Browser for Android for Mainstream Adoption”. Accessed June 11, 2020. https://www.opentech.fund/results/supported-projects/preparing-tor-browser-android-mainstream-adoption/

[82] Mozilla. “Mozilla Research Grants 2019 H1”. Accessed 29 June, 2019. https://mozilla-research.forms.fm/mozilla-research-grants-2019h1/forms/6510

[83] Brave. “Brave Introduces Beta of Private Tabs with Tor for Enhanced Privacy While Browsing”. Accessed June 19, 2020. https://brave.com/tor-tabs-beta/

[84] Facebook. “Making Connections to Facebook more Secure”. Last modified October 31, 2014. https://www.facebookcorewwwi.onion/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237

[85] Facebook. “Making connections to Facebook over Tor faster”. Last modified November 20, 2018. https://www.facebookcorewwwi.onion/notes/facebook-over-tor/making-connections-to-facebook-over-tor-faster/1729157350524311/

[86] Cloudflare Blog. 2018. “Introducing the Cloudflare Onion Service”. Last modified September 20, 2018. https://blog.cloudflare.com/cloudflare-onion-service/

[87] Cloudflare Blog. 2018. “Introducing DNS resolver for Tor”. Last modified May 6, 2018. https://blog.cloudflare.com/welcome-hidden-resolver/

[88] Thali. “Thali and the Internet of Things”. Accessed June 11, 2020. http://thaliproject.org/ThaliAndIoT/

[89] Tor Blog. 2016. "A Quick, Simple Guide to Tor and the Internet of Things (So Far)”. Last modified July 20, 2016. https://blog.torproject.org/quick-simple-guide-tor-and-internet-things-so-far

[90] US Department of State. “DRL Internet Freedom Annual Program Statement for Internet Freedom Technology (Snapshot 14, 2014)”. Accessed June 10, 2020. https://web.archive.org/web/20140113044121/http://www.state.gov/j/drl/p/207061.htm

[91] An overview of such process can be read in 2013 OTF annual report, pp. 26-29.

[92] Vice President Al Gore. “Information Superhighways Speech”. Accessed June 19, 2020. http://vlib.iue.it/history/internet/algorespeech.html

[93] The Framework for Global Electronic Commerce. Accessed June 19, 2020. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/

[94] Global Internet Freedom Task Force. “Homepage”. Accessed June 19, 2020. https://2001-2009.state.gov/g/drl/lbr/c26696.htm

[95] Global Internet Freedom Task Force. “A blueprint for action”. Accessed June 19, 2020. https://2001-2009.state.gov/g/drl/rls/78340.htm

[96] Secretary of State Hillary Rodham Clinton. “Remarks on Internet Freedom”. Accessed June 19, 2020. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

[97] Secretary of State Hillary Rodham Clinton. “Remarks on Internet Freedom”. Accessed June 19, 2020. https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf

[98] US Department of State. “Internet Freedom (Snapshot May 1, 2019)”. Accessed June 19, 2020. https://web.archive.org/web/20190501183236/https://www.state.gov/j/drl/internetfreedom/index.htm

[99] White House. “International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World”. Accessed June 19, 2020. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

[100] Sorcher, Sara and Eaton, Joshua. 2016. “What the US government really thinks about encryption”. *The Cristian Science Monitor*, May 25, 2016. https://www.csmonitor.com/World/Passcode/2016/0525/What-the-US-government-really-thinks-about-encryption

[101] Johnson, Eric. 2016. “Secretary of Defense Ash Carter Supports Encryption Because 'We Have a Serious Concern About Data Security’”. *Re/Code*, March 7, 2016. https://www.vox.com/2016/3/7/11586736/secretary-of-defense-ash-carter-supports-encryption-because-we-have-a

[102] Boyd, Aaron. 2016. “DNI Clapper: Cyber bigger threat than terrorism”. *Federal Times*, February 4, 2016. https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism/

[103] PassCode. 2016. “Cybersecurity Futures 2020”. Last Modified April 29, 2016. https://www.youtube.com/watch?v=C40hwqjRYuI

[104] Elliot, Justin. 2016. “Presidential panel to NSA: Stop undermining encryption”. *Saloon*, December 20, 2016. https://www.salon.com/2013/12/20/presidential_panel_to_nsa_stop_undermining_encryption_partner/

[105] Sankin, Aaron. 2016. “Meet Rep. Will Hurd, the most interesting man in Congress”. *DailyDot*, March 15, 2016. https://www.dailydot.com/debug/will-hurd-sxsw-interview/

[106] Sorcher, Sara and Eaton, Joshua. 2016. “What the US governement really thinks about encryption”. *The Christian Science Monitor*, May 25, 2016. https://www.csmonitor.com/World/Passcode/2016/0525/What-the-US-government-really-thinks-about-encryption

[107] Riseup. “Tor”. Accessed July 5, 2020. https://help.riseup.net/en/security/network-security/tor#riseups-tor-onion-services

[108] Autistici/Inventati. “Tor How-to”. Accessed July 6, 2020. https://www.autistici.org/docs/anon/tor

[109] Systemli. “Onion Services”. Accessed July 6, 2020. https://www.systemli.org/en/service/onion.html

[110] Smith, Adam. 2020. “Signal App downloads soar during George Floyd protests”. *The Independent*, June 4, 2020. https://www.independent.co.uk/life-style/gadgets-and-tech/news/signal-app-downloads-android-iphone-messaging-george-floyd-protests-a9548206.html

4. Privacies

[1] Andreas Pfitzmann (1958 – 2010) is one of the most eminent pioneers of technical privacy protection in the information society. On the site freehaven.net/anonbib – considered as a sort of bible by the crypto freaks all over the world – it is possible to find several many scientific article he wrote (the first one dates back to 1985). For a more detailed account on his life, see Federrath et al, 2011.

[2] While I am writing (September 2018) Torservers include 20 different organizations running relays in 14 countries.

[3] Renewable Freedom Foundation. “Homepage”. Accessed July 10, 2020. https://renewablefreedom.org/. According to its homepage, the organization “aims to protect and preserve civil liberties, especially in the digital landscape” by promoting “the preservation and enforcement of basic human rights and civil liberties via our own research programs, through educational and networking activities, counseling, as well as through direct support of civil society initiatives”.

[4] Hermes Center for Transparency and Digital Human Rights. “Homepage”. Accessed July 10, 2020. https://www.hermescenter.org/. According to its homepage, the organization “to promote and develop awareness and attention to the issues of transparency and accountability within the society”. Its goal “is to increase the involvement of citizens in the management of issues of public interest, and strengthen the active participation of public and private employees in the correct management of the companies they work for”.

[5] Center for the Cultivation of Technology. “Homepage”. Accessed July 10, 2020. https://techcultivation.org/ The organization defines itself as “a "backend provider" for the Free Software community” and its goal is “to become a lightweight scalable fiscal sponsorship "host", much like a payment processor for unincorporated projects”.

[6] Hack This Site! “Homepage”. Accessed July 13, 2020. https://www.hackthissite.org/

[7] Anderson, Nate. 2012. “Stakeout: how the FBI tracked and busted a Chicago Anon”. *ArsTechnica*, July 3, 2012. https://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/

[8] Tor Project. “Homepage”. Accessed July 10, 2020. https://2019.www.torproject.org . It is worth pointing out that nowadays the Tor Project’s official site has undergone significant changes and it presents a completely different aesthetic and structure than those it had taken until 2019.

[9] Tor Project. “Who uses Tor?”. Accessed July 10, 2020. https://2019.www.torproject.org/about/torusers.html.en

[10] Library Freedom Project. “Homepage”. Accessed July 10, 2020. https://libraryfreedom.org/

[11] Tor Blog. 2015. “This is What a Tor Supporter Looks Like: Alison Macrina”. Last modified December 28, 2015. https://blog.torproject.org/what-tor-supporter-looks-alison-macrina

[12] She was not the only one. Many of the people I interviewed have seen in Snowden's revelations a turning point, either personal or, more in general, for the pro-privacy movement.

[13] Guardian Project. 2015. "2015 is the Year of Bore-Sec". Last modified January 2, 2015. https://guardianproject.info/2015/01/02/2015-is-the-year-of-bore-sec/

[14] Woodall, Kermit. 1998. "ThinAirMail. The first "must have" Palm VII software". Pen Computing Magazine July 1998. http://www.pencomputing.com/palm/Reviews/thinair.html

[15] In the IT jargon "forking" means to develop new code from the basis of an existing one.

[16] Guardian Project. 2016. "Copperhead, Guardian Project and F-Droid Partner to Build Open, Verifiably Secure Mobile Ecosystem". Last modified March 28, 2016. https://guardianproject.info/2016/03/28/copperhead-guardian-project-and-f-droid-partner-to-build-open-verifiably-secure-mobile-ecosystem/

[17] Guardian Project. "SQLCipher: Encrypted Database". Accessed July 14, 2020. https://guardianproject.info/code/sqlcipher/

[18] Tor Blog. 2016. "A Quick, Simple Guide to Tor and the Internet of Things (So Far)". Last modified July 20, 2016. https://blog.torproject.org/quick-simple-guide-tor-and-internet-things-so-far

[19] Guardian Project. "Haven: Keep Watch". Accessed July 14, 2020. https://guardianproject.github.io/haven/

[20] Which indeed, despite the disgust publicly expressed by the Tor Project, are hosted on the Tor network (such as the media outlet "Daily Stormer"). See: Tor Blog. 2017. "The Tor Project Defends the Human Rights Racists Oppose". Last modified August 17, 2017 https://blog.torproject.org/tor-project-defends-human-rights-racists-oppose

5. Tor politics

[1] Tor Bug Tracker & Wiki. "Network Team". Accessed August 10, 2020. https://trac.torprject.org/projects/tor/wiki/org/teams/NetworkTeam. According to this page, the Network Team is "a group of Tor people who are working on Tor back-end: the program called Tor, the pluggable transports, the bridge distribution, the network simulators, the scripts that supports directory authorities, onion services

[2] Tor Bug Tracker & Wiki. "Metrics Team". Accessed August 10, 2020. https://trac.torproject.org/projects/tor/wiki/org/teams/MetricsTeam. According to this page, the Metrics Team is "a group of Tor people who care about measuring and analyzing things in the public Tor network"".

[3] Tor Bug Tracker & Wiki. "Application Team". Accessed August 10, 2020. https://trac.torprject.org/projects/tor/wiki/org/teams/ApplicationsTeam. According to this page,

the Application Team is “a group of Tor people who are working on different user facing products: Tor Browser, Tor Messenger, Tor Mail, Orfox”).

[4] Tor Bug Tracker & Wiki. “Community Team”. Accessed August 10, 2020. https://trac.torproject.org/projects/tor/wiki/org/teams/CommunityTeam. According to this page, the aim of the team is “helping people who use Tor, and growing and sustaining the Tor community”.

[5] Tor Bug Tracker & Wiki. “Anti Censorship Team”. Accessed August 10, 2020. https://trac.torproject.org/projects/tor/wiki/org/teams/AntiCensorshipTeam. According to this page, the Anti Censorship team is “a group of Tor people who make Tor reachable anywhere in the world”.

[6] Tor Bug Tracker & Wiki. “Fundraising Team”. Accessed August 10, 2020. https://trac.torproject.org/projects/tor/wiki/org/teams/FundraisingTeam. According to this page, the Fund raising team is ““responsible for raising funds from individual donors, foundations, corporations and other entities who are interested in financially supporting the Tor project and our work”.

[7] Tor Bug Tracker & Wiki. “Ux Team”. Accessed August 10, 2020. https://trac.torproject.org/projects/tor/wiki/org/teams/UxTeam

[8] Inspectlect (https://www.inspectlet.com/) and HotJar (https://www.hotjar.com/) are just two of the most notorious name in a market sector which is constantly growing.

[9] Ideo. “Design Kit: The Human-Centered Design Toolkit”. Accessed August 10, 2020. https://www.ideo.com/post/design-kit

[10] It is worth noting the emphasis put on consent in the feminist principles of the Internet: "We call on the need to build an ethics and politics of consent into the culture, design, policies and terms of service of internet platforms. Women’s agency lies in their ability to make informed decisions on what aspects of their public or private lives to share online”. Feminist Principles of the Internet. “Consent”. Accessed August 10, 2020. https://feministinternet.org/en/principle/consent

[11] Isabella Bagueros. 2018. “Is 2018 and UX will kick ass!! First 2018 week status check in :)”. Mail sent to the Tor UX mailing-list. https://lists.torproject.org/pipermail/ux/2018-January/000384.html

[12] Tor Bug Tracker & Wiki. “Global South”. Accessed August 11, 2020. https://trac.torproject.org/projects/tor/wiki/org/teams/CommunityTeam/Projects/GlobalSouth

[13] Tor Bug Tracker & Wiki. “User Research”. Accessed August 11, 2020. https://trac.torproject.org/projects/tor/attachment/wiki/org/teams/UxTeam/UserResearch/

[14] During the 2019 Tor-dev meeting kept in Stocholm, the UX team strengthen this approach, introducing Personas, a tool for sharing this kind of information across teams in the organization. Tor Bug Tracker & Wiki. “User Personas”. Accessed August 11, 2020. https://track.torproject.org/projects/tor/wiki/org/meetings/2019Stockholm/Notes/UserResearchPersonas

[15] RTFM is an acronym for "read the fucking manual!"

[16] Tor Blog. 2019. "New Release: Tor Browser 8.5". Last modified May 21, 2019. https://blog.torproject.org/new-release-tor-browser-85

[17] Tor Blog. 2019. "New Release: Tor 0.4.0.5". Last modified May 3, 2019. https://blog.torproject.org/new-release-tor-0405

[18] It is possible to find thousands of on-line news and articles about the expulsion of Jacob Appelbaum from the Tor Community (the so-called #JackGate). The following one are among the most comprehensive and complete: enegnei. "Jacob Appelbaum Leaves the Tor". Accessed August 11, 2020 https://github.com/Enegnei/JacobAppelbaumLeavesTor and cjdelisle. "JakeGate". Accessed August 11, 2020. https://github.com/cjdelisle/JakeGate

[19] Jacob Appelbaum. "Homepage". Accessed August 11, 2020. http://jacobappelbaum.net/

[20] Alison Macrina. 2016. "There is really no such thing as the 'voiceless'". Last modified June 15, 2016. https://medium.com/@flexlibris/theres-really-no-such-thing-as-the-voiceless-92b3fa45134d

[21] Ccc.media.de. "The Tor Network. We're living interesting times". Last modified December 31, 2013. https://media.ccc.de/v/30C3_-_5423_-_en_-_saal_1_-_201312272030_-_the_tor_network_-_jacob_-_arma#video&t=1560

[22] Tor Blog. 2015. "Transparency, Openness and our 2015 Finacials". Last modified April 21, 2017. https://blog.torproject.org/transparency-openness-and-our-2015-financials

[23] Horne, Bethany. 2016. "Shari Steele on online anonymity: Tor staff are 'freedom fighters'". *The Guardian*, January 11, 2016. https://www.theguardian.com/technology/2016/jan/11/shari-steele-tor-encryption-online-anonymity-censorship 1, 2016.

[24] Horne, Bethany, 2016. Ibidem.

[25] Turton, William. 2016. "The woman who aims to make Tor mainstream". *Daily Dot*, February 16, 2016. https://www.dailydot.com/debug/shari-steele-tor-project-eff/

[26] Tor Blog. 2020. "The Tor Project Membership Program". Last modified September 1, 2020. https://blog.torproject.org/tor-project-membership-program

[27] Riehle Group. 2016. "FLOSS-2016-05-31 – The center for cultivation of technology (Moritz Bartl)". Last modified November 28, 2016. https://www.youtube.com/watch?v=RDHCFkhHX7I

[28] Ccc.media.de. 2015. "State of the Onion". Last modified December 29, 2015. https://www.youtube.com/watch?v=DqBFez4v_2I

[29] A PT is a technology mostly used in areas under a strict censorship regime where users cannot connect to the Tor network. PTs hide to an external observer (i.e. an Internet Service Provider) the fact that a user is generating traffic directed toward the Tor network and mask it as if it was simple encrypted traffic. There are several PTs currently available: some of them mask the data generated by the user as if it was directed towards big Internet actors (like Amazon or Google) which can be hardly censored. For more information see: Tor Project. "Pluggable Transports". Accessed August 13, 2020 https://2019.www.torproject.org/docs/pluggable-transports.html.en

[30] As reported by Roger Dingledine during the 2013 “State of The Onion”. See: Ccc.media.de. 2013. “The Tor Network. We’re living interesting times”. Last modified December 31, 2013. https://media.ccc.de/v/30C3_-_5423_-_en_-_saal_1_-_201312272030_-_the_tor_network_-_jacob_-_arma#video&t=1560

[31] Ccc.media.de. 2013. Ibidem.

[32] Unfortunately, in June 2020 a situation of this kind has occurred. The Trump administration fired the executives of Radio Free Asia and Open Tech Fund and reallocated funds to other proprietary and closed source anti-censorship projects. While I am writing the situation is still in evolution. More information can be found at https://saveinternetfreedom.tech/

[33] Tor Blog. 2018. “Transparency, Opennes, and our 2016 and 2017 Financials”. Last modified December 8, 2018. https://blog.torproject.org/transparency-openness-and-our-2016-and-2017-financials

[34] Tor Blog. 2019. "Strength in number. The final count is in”. Last modified January 10, 2019. https://blog.torproject.org/strength-numbers-final-count

[35] Tor Blog. 2018. “Hack with us in Mexico City / Hackeá con Tor en México”. Last modified September 7, 2018. https://blog.torproject.org/hack-us-mexico-city-hackea-con-tor-en-mexico

[36] Tor Blog. 2018. “Pune Meetup: Privacy Tools and Technologies”. Last modified August 20, 2018. https://blog.torproject.org/pune-meetup-privacy-tools-and-technologies

[37] Tor Blog. 2018. “Tor Meetup Porto Alegre (Brasil)”. Last modified June 29, 2018. https://blog.torproject.org/tor-meetup-porto-alegre-brasil

[38] Tor Blog. 2017. “Tor en Primavera Hacker este fin de semana en Santiago (Join Tor at Primavera Hacker in Santiago This Weekend)”. Last modified November 29, 2017 https://blog.torproject.org/tor-en-primavera-hacker-este-fin-de-semana-en-santiago

[39] Tor Blog. 2017. “We're Welcoming Two New Members to Our Board of Directors”. Last modified October 10, 2017. https://blog.torproject.org/were-welcoming-two-new-members-our-board-directors

[40] Tor Blog. 2018. “Strength in Numbers: Growing Our Board of Directors”. Last modified November 13, 2018. https://blog.torproject.org/strength-numbers-growing-our-board-directors

[41] Tor Blog. 2018. “Announcing Tor’s Next Executive Director: Isabela Bagueros”. Last modified April 23, 2018. https://blog.torproject.org/announcing-tors-next-executive-director-isabela-bagueros

[42] Tor Blog. 2018. “Tor + Outreachy: Internships for Underrepresented People in Tech”. Last modified February 21, 2018. https://blog.torproject.org/tor-outreachy-internships-underrepresented-people-tech

[43] Tor Blog. 2020. “The Tor Project Membership Program”. Last modified September 1, 2020. https://blog.torproject.org/tor-project-membership-program

[44] Cursano, Roberto, Ovidi, Riccardo and Austa, Giampaolo. 2018. “Italy adopts whistleblowing law in the private sector”. *Global Compliance News*, January 15, 2018. https://globalcompliancenews.com/italy-whistleblowing-20180115/

[45] ISPs are usually inflexible with customers who engage in abuses such as spam and, when these occur, terminate the service

[46] Dingledine's mail announcing the first draft of 2005 Tor Tech Report https://lists.torproject.org/pipermail/tor-talk/2005-February/005073.html

[47] Tor Project. "Press". Accessed August 13, 2020. https://www.torproject.org/press/index.html

[48] Perera, David. 2015. "Foundation of 'dark Web' steps into the light". *Politico*. October 21, 2015. https://www.politico.com/story/2015/10/foundation-of-dark-web-steps-into-the-light-215027

[49] Borland, John. 2013. "For Tor, Publicity a Mixed Blessing". *Wired*, December 28, 2013. https://www.wired.com/2013/12/tor-publicity-mixed-blessing/

[50] O'Neil, PatrickH. 2015. "Tor's great rebranding". *Daily Dot*, March 26, 2015. https://www.dailydot.com/debug/tor-media-public-relations-perception/

[51] DEF CON_Hacking Conference. "Home page". Accessed September 01, 2020. https://defcon.org/

[52] DEFCONConference. "DEF CON 25 – Roger Dingledine – Next Generation Tor Onion Services". Last modified October 13, 2017. https://www.youtube.com/watch?v=Di7qAVidy1Y

[53] The license originally conceived by Richard Stallman in 1989 that appoints the users of the freedom to use, study, share and modify the software.

[54] LaPorte, Leo. 2015. "Triangulation 229: Paul Syverson, Inventor of Tor". Last modified December 15, 2015. https://www.youtube.com/watch?v=_1xbCNyJVzU