

DESIGNING THE FUTURE NETWORKED SOCIETY

Nicola Polverari

Dissertation submitted as partial requirement for the conferral of
Master in Management of Service and Technology

Supervisor:
Researcher Cátia Miriam Costa, Centre for International Studies

September 2018

© Copyright by Nicola Polverari. Student 2018

All Rights Reserved

ABSTRACT

In the past technology innovations paved the way for new general pattern of changes in production and management. Today the Internet is currently the largest network of communication worldwide and is the crucial point where technological innovation could be observed. This phenomenon directly affects economy, business, and society. Internet governance is thus one of the most pressing issue of our time. In the last decade, the attention for think tanks as significant policy-making actors has grown, not in the least because the think tank landscape has developed in such a way that it is hard to ignore their presence and significance.

This dissertation explores through two different case studies what are the different issues that must be tackled in technologies domain, and then developing two different scenarios based on open or closed paradigms. Understanding how the Internet will evolve is critical for researchers and practitioners of innovation, business and management.

No passado, as inovações tecnológicas deram lugar a novos padrões de mudança na produção e gestão da tecnologia. Atualmente, a internet é a rede de comunicação mundial e é o elemento crucial em que a inovação tecnológica pode ser observada. Este fenómeno afecta diretamente a economia, os negócios e a sociedade. A governança da internet é uma das questões mais relevantes do nosso tempo. Na última década, a atenção para com os Think Tanks como atores significativos de políticas públicas cresceu, dado o desenvolvimento que os Think Tanks tiveram, que tornou difícil ignorar a sua presença e significado.

Esta dissertação explora, através de dois estudos de caso diferentes, o que deve ser abordado no que se refere ao domínio das tecnologias, desenvolvendo dois cenários baseados nos paradigmas fechado e aberto de acesso à internet. A compreensão de como a internet irá evoluir é fundamental para investigadores, técnicos de inovação, empresários e gestores.

Keywords: Internet; Technology Innovation; Think Tanks; Network Society.

Keywords: Internet, Inovação Tecnológica; Think Tanks; Sociedade em Rede.

JEL: 032 (Management of Technological Innovation and R&D);

033 (Technological Change: Choices and Consequences – Diffusion Processes).

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to all my professors at ISCTE Business School. In particular I want to thank to my supervisor Cátia Miriam Costa for her comments, criticisms and support throughout this entire process. Thanks to the director of my course, Dr. João Vilas-Boas, for his constant support and indefatigable patience. Moreover, I owe a debt of the deepest gratitude to my fellow students, they made me feel like family. My best wishes to them all in their future endeavors. Last but not least, I dedicate my appreciation to my family. To my parents and brother, your encouragement has been really important. Thank you also for all the people who supported and stand by me during these years.

TABLE OF CONTENTS

	Page
ABSTRACT	vii
ACKNOWLEDGMENTS	v
LIST OF FIGURES	viii
LIST OF ABBREVIATIONS.....	ix
1. INTRODUCTION.....	1
1.1 Literature Review	5
1.2 Research Design	11
1.2.1 Methodological Stance: Realistic.....	11
1.2.2 Research Approach: Deductive.....	11
1.2.3 Research Method: Qualitative.....	12
1.2.4 Research Questions	12
1.2.5 Data Collection	13
1.2.5.1 Primary Data.....	13
1.2.5.2 Secondary Data.....	13
1.2.6 Validity and Reliability of the Research.....	14
2. INTERNET, THINK TANK AND HYPERCONNECTED SOCIETY	15
2.1 The Internet	15
2.1.1 Architecture.....	16
2.1.2 Governance and Policy.....	19
2.1.3 Security and Privacy.....	21
2.1.4 Social	23
2.1.5 Economy	24
2.1.6 Emerging Paradigms and Technology.....	26
2.2 Think Tank	28
2.2.1 Evolved Internet Future for European Leadership.....	31
2.2.1.1 EU FP7.....	31
2.2.1.2 Starting the Debate.....	31
2.2.1.3 Observations	32
2.2.1.4 Next Step Forward.....	33
2.2.2 Global Commission on Internet Governance.....	34
2.2.2.1 Centre for International Governance Innovation and Chatham House.....	34
2.2.2.2 Starting the Debate.....	34
2.2.2.3 Observations	35
2.2.2.4 Next Step Forward.....	36

2.3	Hyperconnected Society	37
2.3.1	Global Digital Landscape	37
2.3.2	Internet of Things	38
2.3.3	Consumer Trust at Risk	41
3.	WHAT WE NEED TO THINK ABOUT TODAY TO HELP SHAPE THE INTERNET OF TOMORROW?	44
4.	CROSSROADS IN THE INTERNET PATH	46
4.1	Open vs. Closed	49
4.2	Centralized vs. Decentralized	53
4.3	Artificial Intelligence vs. Human Intelligence	56
4.4	Freedom vs Control	60
4.5	Spirituality vs. Hyperconnectivity	62
4.6	Privacy vs. Surveillance	64
5.	HOW WILL INTERNET EVOLVE?	67
5.1	Walled Garden	67
5.2	Open Bush	70
6.	CONCLUSIONS	72
	BIBLIOGRAPHY	74

LIST OF FIGURES

Figure	Page
Figure 1.1: Internet Architecture Network.....	19
Figure 1.2: Sensors for Smart Cities, Internet of Things and Beyond. Source: Libelium Smart World.....	41
Figure 1.3: Comparison of Openness by Role in Platform-Mediated Networks. Source: Eisenmann, Parker, Alstyne.....	51
Figure 1.4: Portuguese Internet Service Provider MEO offers for Smartphone Contract.....	69

LIST OF ABBREVIATIONS

EIFFEL: Evolved Internet Future for European Leadership
GCIG: Global Commission on Internet Governance
ICT: Information and Communication Technology
ICANN: Internet Corporation for Assigned Names and Numbers
DNS: Domain Name System
IP: Internet Protocol
IG: Internet Governance
EU FP7: European Union seventh Framework Programme
WSIS: World Summit Internet Society
CIGI: Centre for International Governance
ARPA: Advanced Research Projects Agency
IMP: Interface Message Processor
ARPANET: Advanced Research Projects Agency Network
IANA: Internet Assigned Numbers Authority
TCP: Transfer Control Protocol
UDP: User Datagram Protocol
HTTP: Hypertext Transfer Protocol
SMTP: Simple Mail Transfer Protocol
ISP: Internet Service Provider
POP: Point of Presence
NAP: Network Access Point
MAE: Metropolitan Area Exchange
IOT: Internet of Things
DOS: Denial of Service
AI: Artificial Intelligence
NGO: Non-Governmental Organization
ERA: European Research Area
MEI: Media Entertainment Information
NSA: National Security Agency
OS: Operating System

P2P: Peer to Peer

I2P: Invisible Internet Project

DDOS: Distributed Denial of Service

UKUSA: United Kingdom-United State of America Agreement

SWIFT: Society for Worldwide Interbank Financial Telecommunication

VPN: Virtual Private Network

API: Application Programming Interface

CHAPTER 1

INTRODUCTION

The original creation of the Internet was based on the idea that this network would be formed mainly by multiple independent networks with an arbitrary design. The current Internet is considered as remarkable success of the technology advancement. The Internet platform enabled innovation that far exceeds the original vision of the system as a research instrument. The Internet and associated services today have transformed the lives of billions of people in areas as diverse as democracy, education, healthcare, entertainment, commerce, finance and civil infrastructure. The Internet and the associated services have contributed to the transformation of the world economy. They catalyze new forms of communication, collaboration, creativity and innovation.

In 1991 Jan Van Dijk, developed the concept of network society in his Dutch trilogy book “De Netwerkmatschapji”. Jan Dijk is one of the foremost scholars developing the Network Society approach, a framework that places networks as the marker for understanding richly integrated societies. This concept explains a new type of society where social relations are organized within communication technologies that form a communication network rather than networks typified by face-to-face social relations (Dijk, 1991). Network Society rose to fame for understanding current societal changes and in the 3rd edition strives for a more encompassing framework to account for recent technological developments and their pervasiveness in everyday life. In 1996 the Spanish sociologist Manuel Castells created an ambitious macro theory following the concept developed by Jan Van Dijk. Network Society is a society where the key social structures and activities are organized around electronically processed information network. It’s about social network which process and manage information and are using micro-electronic based technologies (Castells, 2008). Castells’ work makes one immediately engage with his hallmark concept, the “Network Society”, which in 1996 was introduced in the first volume of its now famous trilogy on the economic, societal and cultural aspects of “The Information

Age”. But this idea is just a node in an expanding cluster of other issues that have characterized his work. His writings combine a desire to describe technology seriously as a point of departure for an aspiration to make insights capable of understanding the ultimate guideposts of organized life in society. In his book “The Informational City” the major themes of technology and organization are fleshed out and clearly at play. Here, Castells sets out to understand the process of transformation and the global reach of those post-industrial cities in which science and technology coalesced with new behaviors and norms (“social innovations”). Technologies such as micro-electronics, computer-aided design, optical fibres enables the augmentation of capacity to generate, process, exchange and store information. Moreover, by facilitating the reprogramming of information embodied in materials (ceramics, alloys) and living organisms (genetic engineering), these innovations paved the way for new general pattern of changes in production and management. These changes converged into a new (techno-economics) “paradigm” (Castells, 1989:12-13), the “informational economy”. The emergence of computer-powered and Internet-based networks, rested on the hand of US West Coast youngsters (such as Bill Gates and Steve Jobs), was a triumph of geographically-based social networking, in which entrepreneurs and engineers accepted that they could learn from others and then trial out their own technological solutions to economically valuable problems. The basic unit economics organization in no longer the 19th century entrepreneur, nor the corporation, but the network. This network model of organization is the engine of the new economics order and is itself held together by a cultural code “informing and enforcing economics decisions at every moment in the life of the network”. Castell refers to it with the term “Network Society”.

Internet is today indispensable part of the businesses as most of the businesses processes have been significantly automated by the underlying Internet technologies in business systems, production, development and communication. The current Internet is the most important infrastructure of the digital society that is adapting itself by use of ad-hoc technical solutions that help to meet the demands of the users and devices, applications and services enabling human activities that were not foreseen in its original design. The networking community being aware of the rising

number of seemingly ad-hoc solutions to the technical problems has come to agreement that these problems are of architectural nature and for that reason a general re-design may be needed.

Nowadays, the development of public policies at the national (governments), sub-national (local authorities) and supra-national level (international organizations) is influenced by think tanks. This means that decisions are taken in a context of diffuse decision-making (Weiss, 1982) in which these actors increasingly influence public choices. Non-state actors are generally well structured organizations struggling to maintain a constant dialogue with the institutional world in order to easily verify that their ideas, interests and value are considered and protected. This means that the nature of these actors puts them in a privileged position “outside the government but not just looking in” (Kingdon, 1995). On the one hand, being outside the government means that they do not have the authority to take final decisions, nor a direct responsibility on them; on the other hand, they do not just observe and evaluate the performance of decision makers – through the renewal (or not) of the chain of trust between representative-represented which is typical of democratic systems – but they act in order to influence it more or less directly. Think tanks literature has mainly focused on the US case as a result of the fact that these organizations developed a precise role inside the US policy-making process more than in any other country. In January 2013, the Global Commission on Internet Governance (GCIG) was launched by two of the most influential international think tanks, respectively from United States and United Kingdom: the Centre of International Governance Innovation and Chatham House. GCIG was established in response to trends toward fragmentation of the Internet, with aim offering guidance on how to address new challenges as they emerge. It provides recommendations and practical advice on the future of the Internet. “One Internet” is both the name of their final report and objective, means the creation of one Internet that is protected, accessible to all and trusted by everyone. Thanks to their final report, the commission puts forward key steps that everyone needs to take to achieve an open, secure, trustworthy and inclusive Internet. Since the Nineties, think tanks have known a global diffusion, allowing their analysis also inside the European context. In July 2006, as a group of individual researchers, upon

an initiative of the EC DG Information Society, was established the Evolved Internet Future for European Leadership (EIFFEL) think tank. Their intention was to address questions as to the how such an ambitious goal as defining the Future Internet can be achieved within the context of pan-European and global research. Through their most famous scientific paper “a white paper from the EIFFEL think tank”, they have developed a critical role within the EU vision for the future internet/networked society.

Internet governance has kept growing in importance as stakes has risen. Internet governance is growing at a very rapid pace, and this rapid expansion and the growth of the Internet is causing major concerns, because countries want more control on that, they do not want somebody else to take the lead over it. Why is there so much interest in internet governance and what is at stake? The most important thing is that people don't want other countries controlling their internet, because they fear that in the case of a conflict, somebody else can basically control their internet, and some of the recent conflicts have actually demonstrated how Internet can be used, or can be disrupted in other countries in addition to the kinetic warfare. In 2013 the game changed quite a bit, and that followed Edward Snowden's revelation about widespread and pervasive monitoring of internet traffic by the US Nation Security Agency. This touched off a global response that continues to reshape the debate over who should control the internet policy. This paper has hence attempted to analyze the role that civil society has played within the context of developing countries and the issues of Internet Governance. To this end, the paper discusses not only the role of civil society but also its impact and the implications that its role has had. The paper also looks at the challenges that civil society has faced and will perhaps continue to face.

It is within the spirit of contributing to this important debate about the Information Society that this paper also offers recommendations within the context of research. First of all, in order to have a clear picture, it is fundamental to know what does it mean Internet, what was its status in the past, what were the shortcomings and the vision by EU, through EIFFEL paper “A white paper from the EIFFEL think tank”, and by US and UK GCIG paper “One Internet”.

What has been asserted throughout this thesis, is that the Internet path is in front of six crossroads: choose one respect the other will design a future networked society and different scenarios. What are the different issues that must be tackled in the technology domain according to EIFFEL and GCIG think tanks? What is their strategic vision for the future Internet Governance?

1.1 Literature Review

This chapter highlights the theoretical contributions of this paper and the current state of knowledge in field. In the paper was analyzed each stage of the influence to Internet Governance, from the term “network society” was coined to Evolved Internet Future for European Leadership and Global Commission on Internet Governance. This process aimed at clarifying concepts and the presentation of tools and methodologies.

In 1996 Manuel Castells developed his hallmark concept, the “Network Society”, which was introduced in the first volume of its now famous trilogy on the economic, societal and cultural aspects of the Information Age. But this idea is just a node in an expanding cluster of other issues that have characterized his work. In his book “The Informational City” (1989) the major themes of technology and organization are fleshed out and clearly at play. Here, Castells sets out to understand the process of transformation and the global reach of those post-industrial cities in which science and technology coalesced with new behaviors and norms (“social innovations”). The book’s opening reverberates with the later Castells (1989:1): “A technological revolution of historical proportions is transforming the fundamental dimensions of human life: time and space.” Castell’s research on the “informational city’s as important new phenomenon would soon be scaled up to the level of the entire economy: “Thus, with the revolution in information technology as the material basis of the emerging system, the various features of structural economic transformation that we have identified related closely to each other. In fact, they join together to form a new type of economy that I, along with a growing number of economists and sociologists propose to call the “informational economy” because, at its core, the fundamental source of wealth generation lies in an ability to create new knowledge

and apply it to every realm of human activity by means of enhanced technological and organizational procedures of information processing. The informational economy tends to be, in its essence, a global economy; and its structure and logic define, within the emerging world order, a new international division of labor.” (Castells, 1993). The emergence of computer-powered and Internet based networks was itself also a triumph of geographically-based social networking. Both in term of hardware and software, the success of the microelectronics technological wave rested on the hands of US West Coast youngsters (such as Bill Gates and Steve Jobs). Theirs was a densely connected world, in which entrepreneurs and engineers accepted that they could learn from others and then trial out their own technological solutions to economically valuable problems. This being a process that Von Hippel described as “informal know-how trading” and “knowledge-bartering” (Hippel, 1988). Groups of “hackers, geniuses, and geeks” were instrumental in advancing the Information and Communication Technologies that transformed, and keep transforming, the world economy. These were the: “social and cultural forces that provide the atmosphere for innovation. For the birth of the digital age, this included a research ecosystem that was nurtured by government spending and managed by a military-industrial-academic collaboration. Intersecting with that was a loose alliance of community organizers, communal-mined hippies, do-it-yourself hobbyists, and homebrew hackers, most of whom were suspicious of centralized authority.” (Isaacson, 2014). The momentous changes unleashed by the widespread deployment of the new technologies and correlated governance models. Castells coined the term “Network Society”, since it gives a substantial answer to what comes next: an informational social structure in a globalizing economy powered by ICTs. (Castells, 2010). Castells came to recognize that the new society in the making was, in all dimensions, made up of networks. This what the new social structure is all about: social, organization, institutional, technological networks. The basic unit of economics organization is no longer the 19th century entrepreneur, nor the corporation, but the network. This network model of organization is the engine of the new economics order and is itself held together by a cultural code “informing and enforcing economics decisions at every moment in the life of the network”.

Castells' works influenced management and governance issues from many aspects. He explained that technologies innovations such as micro-electronics, computer-aided design, optical fibres paved the way for new general pattern of changes in production and in management. These changes converged into a new techno-economics paradigm (Castells, 1989:12-13). The momentous changes unleashed by the widespread deployment of the new technologies and correlated governance models has been characterized as the Third Industrial Revolution (Freeman and Louçã, 2001), a process leading to the unfolding of the ICT paradigm (Freeman, 2007). It is the kind of society which has generated and co-evolved with this new techno-economic template that has been best captured by Manuel Castells. In "The Rise of the Network Society that Castells" perspectives came to bear on the media system (Howard, 2011:14). Access and capabilities to navigate the net are a prerequisite to participate in the contemporary life thereby determining exclusion of the self (Scott, 2007) and the nature of inequality in the Informational Age (Mendonca, 2015). The ability to create and govern network is most demanding in terms of communication skills. This is why Castells invested so much in discussing media and new media: "I came to the hypothesis that processes of construction of meaning around the realm of communication were central to the formation of power and counterpower, and that communication was undergoing a major process of transformation in the age of digital technologies and the organizational restructuring of business and government." (Castells, 2016).

Innovation, empowerment and decision-making may be identified as the three fundamental processes in which digital technologies have been instrumental, leading to major transformations in the political, social, cultural and economic realms. These changes are themselves included in broader developments of the global polity at multiple levels, which impact in their turn the governance of digital technologies and networks (Castells, 2001; Cowhey and Aronson, 2009).

"A declaration of the independence of cyberspace" (Barlow, 1996) is one of the best known and popular expressions of political concern on this topic, grounds its sovereignty claim on a lack of legitimacy. According to John Perry Barlow, governments lack legitimacy to intervene in internet affairs. For others, the

organizations, groups, technicians and self-proclaimed representative that have mushroomed in cyberspace within the last few years cannot pretend to be more legitimate to govern or regulate the internet, as they are not elected or designated by governments to do so. Since the beginning of the internet, most circumstances of its history have shown that the problem of legitimacy has not been solved, at several levels: the legitimacy of institutions, among them ICANN or the legitimacy of rules. Following decades of top-down arrangements within an exclusive club of Western countries, the World Summit of the Information Society convened successively in Geneva in 2001 and in Tunis in 2005. It established the Internet Governance Forum, which was intended to foster an inclusive global architecture in information and communication technologies. The first attempts to define the term Internet Governance (IG) were made during the preparatory meeting for the United Nations World Summit on the Information Society. A first common-accepted definition was developed within the Working Group on Internet Governance, a multi-stakeholder group created by the UN Secretary General and was included in the Tunis Agenda for Information Society: “development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet”. This definition highlights several important concepts. First, that all segments of society play a role in Internet governance in their areas of expertise or authority. Second, it emphasizes that principles, norms, rules and decision-making procedures must be shared. And third, that Internet governance is concerned not only with the Internet’s design and administration, but also with its evolution and use, so Internet governance is inherently oriented toward the future and the impact on society. As the history of the internet proceeds, developing more complex levels of communication and organization, the question of internet governance implies more and more actors and commentators. With more and more types of activities relying on the network, the social, political and financial stakes rise higher and regulation becomes critical.

The Internet and the Web are key variables in the growth and internationalization of think tanks, proving public policy institutes with the opportunity to disseminate

research and advocate particular policy outcomes in ways that have never before been possible. The Internet facilitates the promotion of policy think tanks' research and supplies access to a wider audience of policy information consumers. Use of the Web to communicate information is commonplace in North America, Europe and parts of Asia with governments, advocacy groups, universities, and numerous other policy actors using the Web to market their ideas to online audiences (Parent, Vandebeek, and Gemino, 2005). Think tanks are among the institutions the most influence public policy at the global level, both internally and externally (Wiarda, 2015). They are institutions born in civil society and generally supported by private funds; they are a source of ideas and evaluation of policy proposals that need experts, a team and sponsors to maintain their activity (Costa, 2016). In Nicander's words they convert political access to money, money into ideas and ideas into legitimacy. However, they do not tend to be corporatist, since they want to maintain independence as their essential characteristic. Contact networks and reputation are considered as some of the key elements for the success of think tank, and this can only be achieved through autonomy in the face of various interests in society. The action of think tank has become essential in shaping political agendas and has made governments themselves often take up the priorities set by these organizations, taking them as the pressing political issues for governance to resolve (Costa, 2016).

This dissertation deals with the finding of the think tanks group of experts from all over the world working within the program of the EU FP7 project "Evolved Internet Future for European Leadership. EIFFEL think tank has come to agreement that a consideration of a large-scale system such as the Internet need to be carefully observed. The evolution of the Internet is becoming compromised (Trossen, 2005) when the architecture does not allow legitimate concerns to be expressed after its original design. As a result, users, providers and business customers solve their problems in ad hoc ways, adding carbuncles in violation of the original architecture. The present Internet design is taking part within organizations that have historically focused more on engineering than innovative vision and social interactions, but the growth brings the system to a new environment that the original designers may not have envisioned, together with new requirements that must be met. EIFFEL states

that there is a need for evolution as a gradually developing process like for any large-scale system, thus we need to understand the dynamics forcing the changes and devise an architecture forcing that is suited for these dynamics to commerce in runtime. Another consideration is regarding the society and business sphere, because the Internet has become more than a technical artifact. Hence the question of evolving the Internet is not a mere technical one anymore. The most important observation of the EIFFEL think tank is that the future architecture should be designed that allows the Internet flexibility to behave in different ways at different times and in different places depending on the outcome of market selection and social regulation mechanisms (Clark, Solling, Wroclawski, Braden, 2005), whilst retaining levels of performance that render it fit for purpose (Clark and Blumenthal, 2007).

The other paper being part of the literature for this dissertation is “One Internet” developed by Global Commission on Internet Governance think tank. The Commission envisions a world in which the Internet reaches its full economic and social potential, where fundamental human rights such as privacy and freedom of expression are protected online. This optimistic future can only be achieved if there is universal agreement to collectively develop a new social compact ensuring that the Internet continues on track to become more accessible, inclusive, secure and trustworthy. The Commission presents this report with the aim of providing high-level strategic advice and recommendations to policy makers, private industry, the technical community and other stakeholders interested in maintaining a healthy Internet. The Commission framed its work with reference to the working definition of Internet governance, developed by the United Nations World Summit on the Information Society (WSIS) in the Tunis Agenda. Implicit in the definition, wrote in the introduction of this literature review, is the recognition that a large number of diverse tasks are undertaken by various stakeholders. These include developing public policies on issues such as privacy, intellectual property rights enforcement, access and interconnection, as well as technical governance functions such as protocol design and the administration of Internet names and numbers.

1.2 Research Design

In this chapter I shall discuss the research design, establishing the linkage between the research questions and the methodology data collection strategy. I will describe in detail how the research for this dissertation has been performed, the chosen methods and the reason they have been used. Further it addresses the way data has been collected, reliability of the data, and the way it has been analyzed. This dissertation will be based on a literature review, including relevant journal articles and books within the area of Internet governance and think tanks.

1.2.1 Methodological Stance: Realistic

Methodological stance used in this thesis is related to the realistic approach. According to Fisher (2007) “the realist researchers looks for associations between variables and where possible tries to establish chains of cause and effect” (Fisher, 2007). “Typically, research in this mode would involve structuring a problem by breking it into its constituent parts”. The relationship between these parts would then be studied, looking for recurrent patterns and associations (Fisher, 2007). As mentioned by Fisher in realist research the research problem is divided into different parts and then the relationship or associations between them would be gathered and studied. We will use the same approach as we want to gather and analyze if the future Internet will be designed for open or closed innovation technology. We divide our research problem into constituent parts. In establishing cause and effect chain we try to investigate cause studying the main players who play this game: the Internet, Think Tanks, and society.

1.2.2 Research Approach: Deductive

To conduct research we considered two research approaches namely structured and grounded approach. According to Fisher (2007) in a structured approach a structure is imposed on the research based on a preliminary theory, concept or hypothesis. Then that structure can be used to guide the research and also in material

gathering process. On the other side, in a grounded approach all the material is collected without any prejudice and no preliminary conceptual thoughts about what is going to be discovered. Fisher (2007) further states that using a structured approach has the security of knowing the structure and shape of the research before actually going to collect the research material. In our thesis we selected a structured approach for gathering data from different articles, doing a literature review of the relevant material being collected from different scientific articles. And then to build up the conceptual framework which guides the rest of the research for the thesis.

1.2.3 Research Method: Qualitative

According to Fisher (2007) any method Qualitative or Quantitative can be used in the research and it is wrong that realist research means using quantitative research method. So based on that, in our thesis by adopting realist research we use qualitative research method. In order to pursue such analysis relating to technological innovations, Internet, institutions, political, non-state actors and their subsequent exchanges, the methodology used for data analysis is the qualitative research. The qualitative research design, as noted by Vromen (2010:253-254) is responsive to real world problems and empirically based. It is defined as any research that generates results and discoveries in which statistical procedures and other means of quantification are not used.

1.2.4 Research Questions

The Internet is currently the largest network of communication worldwide and is where technological advance could be observed. The original creation of the Internet was based on the idea that this network would be formed mainly by multiple independent networks with an arbitrary design. The Internet is the place where all countries communicate and disseminate information in real time. This phenomenon directly affects economies, business and society.

In the past technology innovations paved the way for new general patterns of changes in production and management (Castells, 2016). Today Internet influences

everything in management, from logistics to production. Its governance is thus one of the most pressing issue of our time. What are the different issues that must be tackled in technologies domain? Will be followed an open or closed design?

1.2.5 Data Collection

For this dissertation both secondary and primary data have been collected.

1.2.5.1 Primary Data

The primary data for this thesis has been collected by using case studies. Case study research excels at bringing us to an understanding of a complex issue or object and can extend experience or add strength to what is already known through previous research. Case studies emphasize detailed contextual analysis of a limited number of events or conditions and their relationships. Researchers have used the case study research method for many years in management and business disciplines. Researcher Robert K. Yin defines the case study research method as an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used (Yin, 1984). During the design phase of case study research, I determined to use two case studies to examine in depth. When using multiple cases, each case has been treated as a single one. Each case's conclusion can then be used as information contributing to the whole study, but each case remains a single case. A useful step in the selection process have been repeatedly refer back to the purpose of the study in order to focus attention on where to look for cases and evidence that will satisfy the purpose of the study and answer the research questions posed. Techniques and tools used for organizing and conducting the research successfully have been through literature review and personal observations.

1.2.5.2 Secondary Data

Secondary data is the data which is collected from other researchers work. Secondary data is mostly obtained from academic journals, scientific articles and

books. In our research we use online databases available through (ISCTE University) Scopus digital library. We found articles and journals by typing different keywords related to this thesis, such as: Internet governance, think tank, network society, open or closed innovation.

1.2.6 Validity and Reliability of the Research

To ensure validity and reliability of this research we tried to choose articles from peer reviewed journals. Mostly the articles are collected from Scopus online library. We tried to avoid collecting information from internet and websites as they consider less reliable.

CHAPTER 2

INTERNET, THINK TANK AND HYPERCONNECTED SOCIETY

2.1 The Internet

The Internet is a global system of interconnected computer networks. It is the infrastructure that carries email, instant messaging, Voice over IP, network games, file transfer and, of course, the Web. When two or more electronics device (e.g. computers) are connected so that they can communicate, they become part of a network. The Internet consists of a world-wide interconnection of such networks, belonging to companies, governments and individuals, allowing all of the devices connected these networks to communicate with each other.

On 4 October 1957, the Soviet Union launched the first man-made satellite into space: Sputnik I. US President Dwight Eisenhower created the ARPA agency, the Advanced Research Projects Agency, in order to regain the technological lead in the arms race. It was 1958 and the first ARPA director, Joseph Licklider, started to think about the potential benefits of an Intergalactic Computer Network through which everyone could quickly access data and programs from any site and thanks to the US would get a country-wide communications system (Licklider, Taylor, 1968). This project would later come together with the idea that Paul Baran at Rand was trying to develop. Rand Corporation is an independent non-profit think tank established in 1948 by Douglas Aircraft Company to offer research and analysis to the United States Armed Forces. Baran was tasked with designing a communications system that could survive a nuclear attack. Baran's analysis indicated that centralized networks had single points of failure that made them vulnerable to attack, rather than being based on an end-to-end chain of connections, Baran proposed dividing messages into blocks, sending them via multiple paths and reassembling them on arrival (Baran, 1964). In the UK, Welsh computer scientist Donald Davies drew the same conclusion. He called his solution "packet switching". Davies and Baran learned from each other's work and decided to collaborate.

Lawrence Roberts, the successors of Licklider at ARPA, led development of the network based on the new idea of packet switching. Initially the idea proposed by Roberts was to have a network of host computers (nodes) in which, following the concept of packet switching, information and data had to travel through several nodes to get from one user to its destination (Roberts, 1968). Each node had to copy and store the data sent until it moves on the next node, where it repeats the process of copying and storing. This may create problems of reliability in the network. Instead of a network of host computers, Wesley Clark, an electrical engineer that worked for Washington University, suggested to Roberts the idea of using separate small computers as a way of standardizing the network interface and reducing load on the local computer. The team working on the idea, the “IMP guys”, developed this special computer: Interface Message Processor (IMP), which we call a gateway or router today (Walden, 2003)

Thanks to this first piece of the Internet equipment ever installed, the network made by ARPA was ready: the ARPANET. This machine served as the first node of the Internet for decades and it was from here that the first message was sent: a revolution began. On 29 October 1969 at 10.30 at night, the first communication was made between computers at the University of California (Los Angeles) and the Stanford Research Institute. The first message typed was LOG, because they wanted to do a LOG IN, but the SRI computer crashed, so the first message was LO: used to call attention or to express wonder or surprise.

Known as ARPANET this was the world’s first packet switching network and the first step towards what we know today as The Internet.

2.1.1 Architecture

Today, the Internet has evolved from U.S. military system prototype into an open, world-wide infrastructure over which a rich set of applications, including Web, instant messaging, Voice over IP (VoIP), network games, file transfer are deployed.

On the Internet, communication is possible because all devices use the same “language” or protocol, namely the Internet Protocol (IP), a “single market” with no physical, technical or national barriers. It forms the basis for all other systems of

communication on the Internet. The IP is a numerical address that is assigned to every device connected to the Internet and it is made up of four bytes of information, totaling 32 bits, (Postel, 1981) expressed as four numbers between 0 and 255 shown separated by periods (example 162.29.221.6). The authority with the responsibility of managing the allocation of IP addresses and coordinate the Domain Name System (DNS), which maps text names to IP address automatically (Rekhter, Li, 1993), core resources and protocols of the global Internet, is the Internet Assigned Numbers Authority (IANA), a department of ICANN (Internet Corporation for Assigned Names and Numbers) a not-for-profit private American corporation.

Two types of end-to-end communication services were then defined over IP: Transfer Control Protocol (TCP) which was concerned with service feature such as flow control and recovery from lost packets (Rkhter, Moskowitz, Karrenberg, Groot, Lear, 1996), and for those applications that did not want the services of TCP, an alternative called the User Datagram Protocol (UDP) was added in order to provide direct access to the basic service of IP. Every computer in order to communicate on the Internet needs to go through a protocol stack that is built into the computer's operating system (i.e. Windows, Mac OS, Unix, etc.). The protocol stack used on the Internet is referred to as the TCP/IP protocol stack because of the two major communication protocols used. The protocol stack is composed by:

- Application Protocols Layer: is the layer that most network users are exposed to, and is the level at which human communication happens. Specific protocols to applications such as HTTP for accessing web sites, SMTP for sending emails etc. The human sits above this layer, interacting with the application;
- Transport Protocol Layer: Example of protocols that operate at this layer are TCP and UDP. Some protocols at the transport layer (such as TCP) ensure that all of the data has arrived at the destination, and is reassembled and delivered to the next layer in the proper order;
- Network Protocol Layer: the IP is the most common network layer protocols that has the job to direct packets to a specific computer and reach it thanks an unique IP address;
- Hardware Layer: Converts binary packet data to network signals and back;

Two computers can be connected either physically (Ethernet cable) or wirelessly (WiFi). Such network is not limited to two computers, but you can connect as many computers as you wish but it gets complicated quickly if you are trying to connect ten computers, for instance. To solve this problem, each computer is connected to a special tiny computer called a router. This router has only one job, it makes sure that a message sent from a given computer arrives at the right destination computer. Each router is connected to the public telephone network through dial-up connection that send the signal to a pool of modems maintained by Internet Service Provider (ISP) who provides services for accessing, using or participating in the Internet (Hubbard, Kusters, Conrad, Karrenberg, Postel, 1996). After the signal traverse the pool of modems, is managed by some form of computer (usually a dedicated one) which controls data flow from the modem pool to the ISP's backbone. The Internet backbone is a conglomerate of multiple very high bandwidth networks composed by fiber optic, although some ethernet segments on lower traffic backbone links also exist, and owned by governments, corporations, large organizations, and other Internet service providers. Their technical infrastructure includes global connections through underwater cables and satellite links to enable communication between countries and continents.

The vast majority of computers owned by individuals or businesses connect to the Internet through commercial Internet Service Providers (ISPs). In every region ISPs service, they have a Point of Presence (POP) that has the hardware needed to connect the customer's computer to the ISP. The ISPs are further divided into a three tiers system, from bottom to the top:

- Local ISP (tier 1): they provide or sell services to local homes or companies;
- Regional ISP (tier 2): provide or sell access to Local ISP and interconnect with tier 3;
- National ISP (tier 3): they are the backbone of the internet service provider and they connect to the internet directly and interconnect each other through NAP (Network Access Points) or MAE (Metropolitan Area Exchange) thanks to different ISPs can communicate and exchange packet traffic between them;

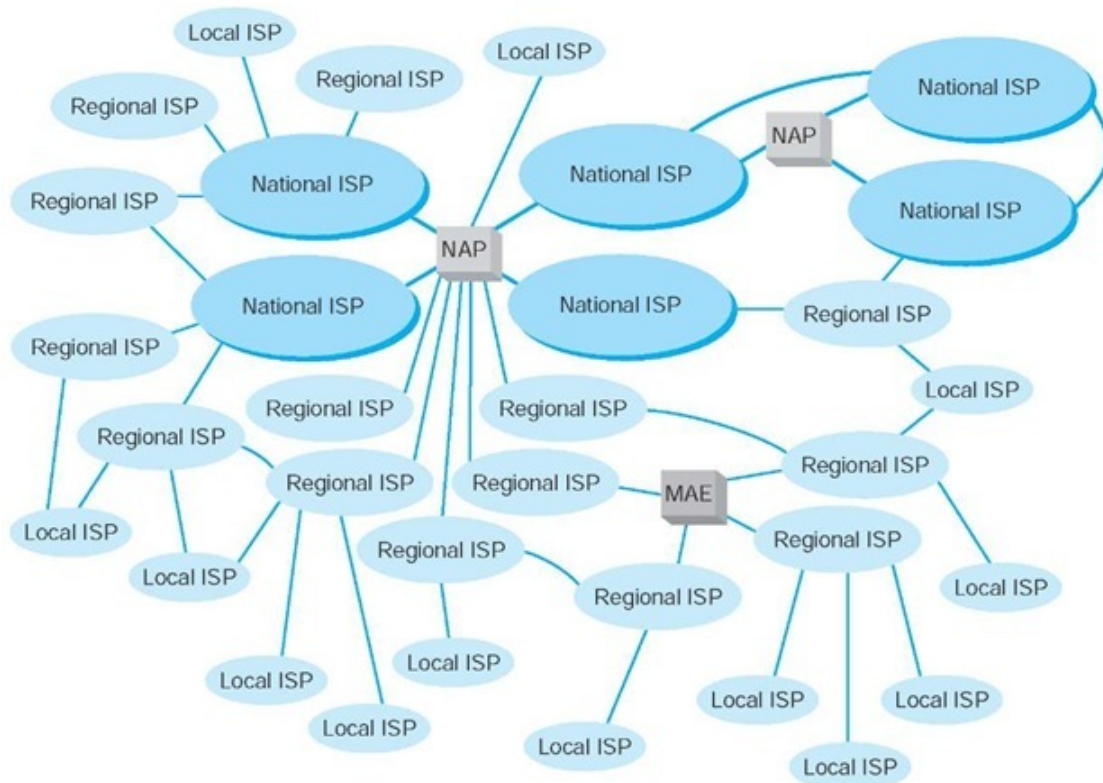


Figure 1.1: Internet Architecture Network. Source: what-when-how.com

2.1.2 Governance and Policy

Internet Governance is the most debatable issue of recent times. The issue emerged as soon as it was realized that the Internet is able to offer global skills of communication and options for free trade (Shahin, 1999).

The first attempts to define the term Internet Governance (IG) were made during the preparatory meeting for the United Nations World Summit on the Information Society (WSIS), in 2005: “development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet”. This definition acknowledges that the development and future of the Internet lies in the collective efforts of a divergent group of participants. The Tunis Summit also recognized the dynamic character of the Internet, and expressed the need

to create a framework and mechanisms to deal with merging issues of Internet Governance and the need to follow the exponential growth of the medium. Moreover, the participants at the Summit recognized that Internet Governance is not limited to Internet naming and addressing, namely ICANN, and that the status of ICANN is only a small fraction of a much bigger issue, which includes other issues with policy implications, such as security of communications, the development of Internet resources and the education of its users.

The most crucial recognition of the Summit can be seen in the acknowledgement that all governments should have an equally active role and responsibility for international governance, a premise which might pose problems to the current governance status, if we accept that ICANN is accountable to the United State Department of Commerce, which would automatically place the United State Government in charge of the Internet. The particular and pivotal position of some actors as gatekeepers makes them able to act as control points in the internet space or as governments' instruments of law enforcement. ICANN, a key gatekeeper, has a central authority over the internet through its management of the Domain Name System (DNS) and Internet Protocol (IP) addresses, a critical resource. Other important gatekeepers include network operators, internet service providers (ISPs), search engines and, most recently, companies owning social networks.

Despite agreement on important aspects, following the Tunis Summit there was still no consensus on the model that should be finally be adopted. The complexity of this heterarchy - a system organization where the elements of the organization are unranked - defines multiple orders, leading to the need to organize their self-organizations. This implies mutual recognition and mutual legitimation between all actors, leading to a reordering of the process of norm-making, and defining net patterns of interactions, through cooperation, co-elaboration and other forms of interaction between the whole range of social and political actors. In the field of Internet Governance, two main ordering principles are witnessed: through the acquisition of new legitimacies and through reflexive governance.

The reflexive self-organization of independent actors involved in complex relations of reciprocal interdependence, with such self-organization being based on

continuing dialogue and resource-sharing to develop mutually beneficial joint projects, and to manage the contradictions and dilemmas inevitably involved in such situations. Dialogue thus appears as an essential element in the Internet Governance process.

2.1.3 Security and Privacy

Nowadays the Internet permeates through every aspect of our corporate, personal and government lives. The Internet is widely perceived as a tool that has given voice to the voiceless, enabling individuals to author their own lives and to share their experiences with a vast network of people around the globe. The term “Internet revolution” refers to the birth of a new information era that has transformed the way we create and share content and where security and privacy protection will become even more necessary in the next five years as we continue to digitize every aspect of our live: the latest “Internet of Things” (IoT).

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol. Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. At the high level, we can say that security has the goal to protect three main properties of data and systems:

- Confidentiality: keeping data users accessible only to them, for instance through encryption;
- Integrity: making sure/verifying that data has not undergone improper or unauthorized change. This also includes verifying the origin of the data. Integrity is often achieved through use of cryptographic primitives, for instance signatures;
- Availability: keeping some system running and reachable by its customers, or keeping some data available to authorized users. Techniques such as firewalls help in this case;

Not every security problem will violate all three security properties, and often there will be variations to the problem that violate different sets of properties.

The issues of privacy and personal data protection have frequently been in the news in recent years, especially in the context of social networking, consumer profiling by online advertising companies and cloud computing. Privacy in an online context includes the right of an individual to (Hughes, 1993):

- Determine what information is collected about them and how it is used. Cookies or information given during a website registration could be sold to third parties that the user even knows;
- Access information held about them and know that it is accurate and safe;
- Anonymity;
- Send and receive e-mail messages or other data that will not be intercepted or read by persons other than intended recipients. Encryption is one way of ensuring this;

Personal data means any kind of information that can personally identify an individual or single them out as an individual (name, address, credit card number, fingerprints, IP address etc.). Personal data is not just information that can be used to identify individual directly, but it is enough if a person is single out from among other people using a combination of pieces of information or other identifiers. For instance, online advertising companies use tracking techniques and assign a person a unique identifier in order to monitor that person's online behaviour, build their profile. Such an advertising company does not need to know that the person in question is but just that user repeatedly visits certain websites, likes determine items etc.

The amount of data growing exponentially brought us to the "Big Data" era. Big Data is the popular description of the accumulation of vast and complex information databases, information that permits organizations (private, public or governmental) to create information about data that were never apparent or intended in the source of information. Processing reliable data can help discover certain trends, which can contribute to reducing the waste of resources and improve policy-making. However, data can also be used to put people under complete surveillance, in breach of their fundamental rights.

2.1.4 Social

The Internet has enabled new forms of social interaction, activities, and social associations. The Internet has always held the promise of expanding access to information and building an open and opportunity-rich society. It empowers individuals to connect, speak, innovative, share, be heard, and organize. From the beginning of the Internet founding fathers, Vint Cerf, believed that a society would emerge from the Internet – an “Internet society”. At the same time, there is an increasing awareness that the Internet’s promise as a force for good may be fundamentally undermined going forward, a result of increasing cyber threats and governments’ reactions to those threats, as well as decreasing levels of trust in the Internet.

The increased use of digital media is changing people’s everyday lives and the way they connect and collaborate in the broader societal context, at work and in civil society. It is enabling unprecedented levels of communication, social interaction and community building across boundaries of time, place and social context.

Social Media are fundamentally different from regular media as they do not just give information, but interact with you while giving you that information. Any website that invites visitors to interact with the site and with other visitors can be considered as part of social media. They can be divided broadly into six different types:

- Collaborative projects where users interact by adding articles and editing existing articles (e.g. Wikipedia);
- Blogs and microblogs (e.g. Twitter);
- Content communities where users interact by sharing and commenting on photos or videos (e.g. Youtube);
- Social networking sites (e.g. Facebook);
- Virtual game worlds (e.g. World of Warcraft);
- Virtual social world (e.g. Second life);

Protection, in particular privacy protection, of social media users is an important topic. As this global Internet emerges, we should not be surprised that the problems in society are finding their way online. As Vint Cerf noted, the Internet is like holding

up a mirror to society, with all of the good and bad that goes with it (Cerf, 1986). It is important to understand the opportunities and the risks, so that both industry and users can learn how best to exploit the benefits while mitigating the negatives effects.

Benefits and opportunities:

- Facilitate social interaction and empowers people
- Gives people a voice, increases civic participation and facilitates the creation of communities
- Changing how work gets done, boosting productivity and enhancing flexibility for workers and employers
- Facilitate education and life-long learning to build and source the skills of the future

Downsides and risks:

- Can be used by communities with harmful intentions to spread propaganda and to mobilize followers;
- By selecting what information reaches which users, digital media can alter human decisions and pose risks to civil society;
- Transformation of work brought about by digital, media may increase inequality and lower productivity;
- Weaken social skills;
- May facilitate bullying, harassment and social defamation;
- May facilitate addiction;
- Benefits of digital media for young children are limited, when used extensively and without guidelines;

The challenge for the Internet going forward is whether society can harness the power of technology and the ingenuity of the private sector to develop norms of behavior so that people can interact safely within their networked communities.

2.1.5 Economy

Since the day the first domain was registered in 1985, the Internet has not stopped growing. It has sailed through multiple recessions and one near-collapse and kept on

increasing in use, size, and impact. The growth is being fueled in large part by two factors: more users and faster, more ubiquitous access. The number of users around the globe is arise to 4,156,932,140 billion. Broadening access, particularly via smartphones and other mobile devices, and the popularity of social media are further compounding the Internet's impact (Anke and Sundaram, 2006).

At the beginning the Internet was an important tool for improving communication, but nowadays is a ubiquitous technology supporting all sectors across the economy. The Internet affects the everyday activities of individuals, companies and governments in numerous ways, but also tends to produce broad, economy-wide effects (Prasad, 2010). The Internet economy has low barrier to entry, and so it is expanding rapidly. Since the Internet ecosystem growing up both technologically and in population, it will be even easier and likelier for countries, companies, and individuals to participate in the Internet economy.

One of the major economic impacts of Internet is its contribution to competitive advantage enabling the following competitive factors:

- Lower search costs for buyers: e-markets reduce the cost of searching for product information (e.g., sellers, models, prices, etc.), frequently to almost zero. This aspect has a huge impact in competition, enabling customers to find cheaper (or better) products and to reduce prices and/or improve customer service;
- Speedy comparisons: Not only can customers find inexpensive product online, but they also can find them quickly. Companies that sell online and provide information to search engines will gain a competitive advantage;
- Lower prices: Companies can offer low prices due to their low costs of operation (no physical facilities, minimum inventories, etc.);
- Customer service: Amazon.com and Dell, for example, provide superior customer service and such service is an extremely important competitive factor;
- Barriers to entry and reduced: Setting up a web site is relatively easy, fast, and inexpensive, and doing so reduces the need for a sales force and brick-and-mortar stores. Companies have to view this as both a threat and as an opportunity;
- Virtual partnership multiply: With access to a World Wide Web of expertise and the possibility to share production and sales information easily, the ability of a

firm to create a virtual team to exploit an e-commerce opportunity increases dramatically;

- Market niches abound: Without the limits imposed by physical storefronts, the number of business opportunities is as large as the Web;
- Differentiation and personalization: Differentiation involves providing a product or service that is not available elsewhere, while personalization refers to the ability to tailor a product, service, or Web content to specific user preferences;

The Internet economy will evolve substantially over the next ten years, fueled by innovations in technology and business models. Advances such as the Internet of Thing (IoT), Artificial Intelligence (AI), and blockchain could bring about an industrial and technological “renaissance”. In a hyperconnected economy, no sector of the economy will be untouched by technology – hospitals, transportation companies, manufacturing firms – and only those who adapt quickly to technological change will be successful.

2.1.6 Emerging Paradigms and Technology

The Internet has tremendously evolved in the last few years. With the advancement in technology, we are moving towards a society where everything and everyone will be connected (Zheng, Simplot-Ryl, Bisdikian, Mouftah, 2011:11), with the convergence of the Internet and physical worlds and the deployment of the Internet of Things (IoT).

The IoT consists of a network of physical devices, vehicles, home appliances, and other items embedded with sensors, and connectivity which enables these things to connect and exchange data between real world devices and applications (Yu, Wang, Zhou, 2010). The IoT links real life and physical activities. The IoT is considered as the future evolution of the Internet that realizes machine-to-machine (M2M) learning (Huang, Li, 2010). However, increased security threats and device vulnerabilities, as well as incompatible standards and a lack of interoperable systems, could well undermine the technology’s promise. Without appropriate safeguards and deliberate

efforts to ensure transparency and user control, IoT could drive data collection and use in ways that further undermine privacy.

Another major paradigm is the Artificial Intelligence (AI). Artificial intelligence is that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment (Nilsson, 2001). For most of its history, AI research has been divided into subfields that often fail to communicate with each other. These sub-fields are based on technical considerations, such as particular goals:

- Large-scale machine learning: a major focus of current efforts is to scale existing algorithms to work with extremely large data sets;
- Deep learning: the ability to successfully train convolutional neural networks has most benefited the field of computer vision, with applications such as object recognition, video labeling, activity recognition, and several variants thereof;
- Reinforcement learning: focus on decision making, and is a technology that will help AI advance more deeply into the realm of learning about and executing actions in the real world;
- Robotics: how to train a robot to interact with the world around it in generalizable and predictable ways;
- Computer vision: for the first time, computers are able to perform some visual classification task better than people. Actually many research are focused on automatic image and video captioning;
- Natural Language Processing: developing refined and capable systems that are able to interact with people through dialog, not just react to stylized requests;

The advent of Artificial Intelligence promises new opportunities, ranging from new services and breakthroughs in science, to the augmentation of human intelligence and its convergence with the digital world. AI has important potentiality, but voices of concern about its unfettered development without appropriate human-centred safeguards are growing. In particular, ethical considerations must be prioritized in the design and deployment of AI technologies.

The nature of blockchain technology, along with its capacity to maintain an exponential historical record of information at a massive scale, has led to a

heightened adoption. Blockchains are distributed ledger systems-that is, information is store not in a single, centralized database, but in a potentially infinite number of places. Blockchains store immutable records and they are distributed among every user, each of whom has their own private cryptographic key. Blockchain technology is changing the way finance, trade, and commerce are done, and it can be used for streamlining many more business processes outside the financial domain. Blockchain is able to combine the openness of the Internet (decentralized system) with the security of cryptography.

The future Internet is grounded in the technological infrastructure for advanced networks and applications. It constitutes a complex and dynamic system and societal phenomenon; it compromises the processes of innovation, shaping and the actual use of these technologies and infrastructures in private and public organizations, in different sectors of the economy including the service sector, and in social networks.

2.2 Think Tank

Policy actors such as university researchers, think tank policy advocates, and lobby groups such as NGOs, unions, the media, industry, society and the community, have all, at some stage or other, played a role in the public policy process. This has resulted in various types of networks being formed between non-state actors in the policy space (Weiss, 1982).

In the last decade, the attention for think tanks as significant policy-making actors has grown, not in the least because the think tank landscape has developed in such a way that it is hard to ignore their presence and significance. This success is in line with the profound changes that the states have introduced in governance, particularly with the disinvestment and erosion of the internal capacity of the Public Administration to generate medium and long-term ideas, raising the problem of strategic thinking which, in the image of other issues, before being delivered to the public sector, were sent to outsourcing (Stone, 2000). It was this breakdown of the governmental monopoly, based on the reduction of State budgets, which allowed

these thinkers to come from the private sector, with such a dimension that it became one of the reasons for its success.

Think tanks mission is to act as bridge between the academic and policymaking communities and between states and civil society, serving in the public interest as independent voices that translate research into a language that is understandable, reliable, and accessible for policymakers and the public. The actions and activities of Think Tanks has become essential in shaping political agendas and has made governments themselves often take up the priorities set by these organizations, taking them as the pressing political issues for governance to resolve. In this way, Think Tanks can claim for themselves the identification of a problem or the opportunity to implement a new policy, putting them at the forefront of certain political-state agendas. But what are Think Tanks? Think tanks are public-policy research analysis and engagement organizations that generate policy-oriented research and advice on domestic and international issues, thereby enabling policymakers and the public to make informed decisions about public policy. Think tanks may be affiliated or independent institutions that are structured as permanent bodies, not ad hoc commissions. (McGann, 2017). In the global context, most think tanks can be classified into broad categories, each one as different kind of financing aspect:

- Autonomous and independent: Significant independence from any one interest group or donor and autonomous in its operation and funding from government;
- Quasi independent: Autonomous from government but controlled by an interest group, such as donor, that provide funding and have thus significant influence over them;
- Government affiliated: means that work closely with the government;
- Quasi governmental: funded exclusively by government grants and contracts but not a part of the formal structure of government;
- University affiliated;
- Political party affiliated: close relationship with political party;
- Corporate (for profit): a for-profit public policy research organization, affiliated with a corporation or merely operating on a for-profit basis.

Western societies, since the Enlightenment, have been confronted with initiatives by civil society aimed at influencing political decision-making. The Academies of Sciences and the Royal Societies of knowledge were institutions in which we can now recognize the same principles of Think Tanks: they also sought to inculcate public opinion in order to change public policies. As today, and not without their connection to the university, these institutions were converting academics and non-academics to the issues they wanted to see treated politically. They used their good offices with political actors to create influences in the name of science, rationality, and ethics. In this respect, they differ little from what is the current reality of Think Tanks and their relation to the academic world. Today, think tanks have broader arsenal in order to exercise influence:

- Through events for journalists, congresspeople, policymakers, and other think tankers;
- Television and media;
- Public appearances, such as lectures around the country, briefings for government officials, journalists;
- All the large think tanks have high-level advisory panels (CEOs, government officials) who help guide their programs, give advice, and provide access;
- Personal contacts;
- Almost all think tanks are staffed with former government officials who use their connection to gain access to policy makers or help their colleagues secure such access;
- Studies and publications;
- All of the think tanks have gone high-tech, with their own media offices, flashy websites, chat rooms, targeted email lists, rapid-response hot lines, Twitter accounts, Facebook pages, blogs, and other social media tools.

However, these academics are exempt from fulfilling some of the requirements of scientific production. Thus writing Think Tanks documents becomes more attractive, being direct, accurate and clear and making recommendations at the end, keeping in mind that the reader, listener or viewer of your communication will be a journalist, politician or ordinary citizens. The nature of these actors puts them in a privileged

position “outside the government but not just looking in” (Kingdom, 1995). On the one hand, being outside the government means that they do not have the authority to take final decisions, nor a direct responsibility on them; on the other hand, they do not just observe and evaluate the performance of decisions makers, but they act in order to influence it more or less directly.

2.2.1 Evolved Internet Future for European Leadership

The Evolved Internet Future for European Leadership (EIFFEL) think tank was established in July 2006 as a group of individual researchers, upon an initiative of the EC DG Information Society, with the intention to address questions as to the how such an ambitious goal as defining the Future Internet can be achieved within the context of pan-European and global, research.

2.2.1.1 EU FP7

The 7th Framework Programme for Research and Technological Development (FP7) is a funding programme create by the European Union/European Commission to support and foster research in the European Research Area (ERA) from 2007 until 2013. Indeed, FP7 is an important tool to respond to Europe’s needs in terms of jobs and competitiveness, and in order to improve leadership in the global knowledge economy. The total budget, €50 billion, will be spent on grants to research actors all over Europe, so as to co-finance research, technological development and demonstration projects.

2.2.1.2 Starting the Debate

The Internet has become a critical communication medium that is progressively reaching its technical limits. It has recognized shortcomings in areas including security, resiliency/robustness, accountability, mobility and manageability. These shortcomings, if they remain unaddressed, will seriously impact the society’s ability to utilize and exploit the Internet in the future.

One of the key findings by several study groups, the EIFFEL think tank among them, is the need for a balanced research agenda. In this balanced approach, the following list of potential technical areas is expected to attract interests:

- Future architecture;
- Security, privacy and rules enforcement;
- Emerging paradigms and technologies;
- Governance and policy aspects;
- Societal, sociological and economical aspects;

2.2.1.3 Observations

The EIFFEL think tank believes that taking into account the large amount of different issues that must be tackled, not only in the technology domain, but also in governance, policy and business, it may be better not to refer simply to the “Future Internet”, but to the “Future Networked Society”. The required scope for the white paper realized by EIFFEL, is very wide but I summarize the main aspects below:

- Technology: the need for an appropriate balance between evolutionary and truly high risk – high gain revolutionary research. Technology research needs to be intensified, but not by forgetting the other aspects;
- Policy and governance: there has been tendency to leave these issues to be handled after the technology has been developed. In the case of the global networked society, this is not a desirable approach;
- Socio-economics aspects: the sociological aspects are, naturally, related also to policies and governance models. As we are moving towards an information-drive society and networking capability becomes pervasive, it is important that socio-economics aspects are considered not only as “lip service”, but in true research fashion. Moreover, there should be mechanism to generate discussion by the users and citizens themselves;
- Business considerations: the future network needs to be built upon the foundation that it can be used for commercial purpose and will be run by commercial organizations under the oversight of proper governance and policy rules. The

economical and commercial issues need to be taken into account. That said, those considerations should not become a hurdle to innovation;

2.2.1.4 Next Step Forward

The most important observation of the EIFFEL think tank is that the future architecture should be designed in order to allow the Internet flexibility to behave in different ways at different times and in different places depending on the outcome of market selection and social regulation mechanisms, whilst retaining levels of performance that render it fit for purpose.

Some of them as identified by the EIFFEL think tank can be:

- Resilience, failure tracking and management: the internet's distributed design is popularly renowned for its robustness to failure. The result is an increasingly unreliable service;
- Availability and robustness to attack: The Internet is continually being used as the means for malware to attack both services and the Internet infrastructure itself. Proper architectural support to address the root means of these attacks is needed;
- Information security scalability: the techniques do not scale to global proportions in non-hierarchical groups. Once the information has been shared at all, any control is essentially lost of any further sharing and exposure;
- Resource accountability: network operators are deploying boxes to limit or block communication with certain users or by certain applications. The consequent inability to properly limit free riding leads to uncertainty over whether capacity investments can be recouped, which in turn negatively affects the whole value chain of the Internet;
- Network-application coordination: the application programming interfaces (APIs) at the top of the TCP/IP protocol suite have become ossified and scale, but more importantly they have become almost impenetrable;
- Scaling for more extreme dynamics: the dynamic range of the Internet architecture is hitting its limits;

2.2.2 Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) was launched in January 2014 by the Centre for International Governance Innovation (CIGI) and Chatham House in response to trends toward fragmentation of the Internet, with the goal of offering guidance on how to address new challenges as they emerge.

2.2.2.1 Centre for International Governance Innovation and Chatham House

The Centre for International Governance Innovation is an independent, American, non-partisan think tank with an objective and uniquely global perspective. CIGI supports research, suggest policy debate and generates ideas for multilateral governance improvements: global economy, global security and politics, and international law.

The Chatham House, the Royal Institute of International Affairs, is an independent policy institute based in London, with the mission to analyze and promote the understanding of major international issues and current affairs. Chatham house engages governments, the private sector, civil society, and its members to carry out independent study of critical global, regional and country-specific challenges and opportunities.

2.2.2.2 Starting the Debate

Upwards of one billion new users and 20 billion devices are forecast to be online within five years. However, for this future to deliver its promise of greater digital freedom, security, trustworthiness and accessibility for all, governance of the Internet across all its dimensions must be an obvious priority around the world (Leymann, 2005). It is vital that the rules and safeguards of Internet governance keep up with the pace of digital innovation, particularly in the sphere of the IoT. At the same time, the process of governance must not inadvertently slow down the spread of the Internet's benefits, reduce creativity or inhibit its global reach.

2.2.2.3 Observations

The Commission envisions a world in which the Internet reaches its full highest potential, where fundamental human rights such as privacy and freedom of expression are protected online. This goal can only be reached if everyone make an effort to develop a new social compact in order to maintain, and make the Internet more accessible, inclusive, trustworthy, and secure.

- Open Internet: the network needs to remain open, allowing data to flow freely based upon the architectural principle of efficiency and non-discrimination. Free expression is a fundamental human right and the foundation for innovation to take place (Clark, 2005). Governments must resist initiatives that are harmful to the basic rights of people and detract from the innovative potential of the Internet;
- A secure Internet: Personal freedom, economic growth and innovation, particularly in the IoT, will be degraded if the digital space is not sufficiently secure and all actors do not practice better digital “hygiene.” Governments should not absolutely build back doors or compromise encryption standards, as these efforts would weaken the Internet and fundamentally undermine trust. Efforts by the technical community to incorporate privacy-and-security-enhancing solutions into all standards and protocols of the Internet should be encouraged;
- A trustworthy Internet: There is a need to reverse the erosion of trust in the Internet brought about by indiscriminate and non-transparent private practices such as the collection, integration and analysis of vast amount of private information about individuals, companies and organizations;
- An inclusive Internet. Governments should use competition as a tool to expand Internet access facilities to the maximum extent possible, while investing to ensure availability when market forces prove insufficient. Public investment in schools and libraries can provide wider access to communities with limited opportunities.

2.2.2.4 Next Step Forward

The Commission mandate is built in order to advance strategic vision for the future of Internet governance considering the actual global political challenges. In light of these challenges, the Commission's report suggests a series of recommendations, towards creating a more open, secure, trustworthy, and inclusive Internet. The recommendations are wide-ranging:

- Net neutrality: Recognizing net neutrality as a key principle to help preserve the Internet's accessibility (Huston, 2006), the Commission makes relevant recommendations to further this principle, for instance sanctioning non-neutral practices such as blocking, filtering, and zero-rating;
- Mass surveillance: Commission recommends that "Interception of communications and collection and analysis of data over the Internet by law enforcement and government intelligence agencies should be for legitimate purpose, openly specified in advance, authorized by law and requiring the application of the principles of necessity and proportionality";
- Privacy and data protection: Since users' privacy is threatened not only by official surveillance but also by commercial data collection, the Commission recommends that users of online services "should know about and have some choice over the full range of ways in which their data will be deployed," and that "To assure the public that their data is being appropriately protected, states that do not already have comprehensive personal data protection legislation and a privacy enforcement authority with legal enforcement powers should take steps to create such regimes.";
- Intermediary liability. The commission fully support the legal principles of "shielding intermediaries from liability for third-party content; the requirement of judicial authority for content takedowns; necessity and proportionality; clarity and due process; and transparency and accountability";
- Encryption. "Governments should not create or require third parties to create "back doors" to access data that would have the effect of weakening the security of the Internet," and further notes that "State should not rely upon the weaker data

collection rules that govern private companies to get access to information that they could not obtain themselves through legal channels.”;

2.3 Hyperconnected Society

Hyperconnectivity refers not only to the technology that enables communication and interaction, but also to the impact that this technology has on personal lives, business, government and societal behavior (Cheok, 2015). Hyperconnectivity derives from a combination of the wider availability of broadband Internet expansion, the growing of the number of mobile and wearable computing devices and wireless Internet access always more performance. It includes the dominance of social media and consumer generated media in daily life and recently, the use of the cloud for only human-to-human formats, but also communication between people and machines and between machines and machines without any direct human involvement.

The phenomenon of instantly available and easily accessible information has created what many are calling “re-wiring” of the human brain. Throughout history, humans have responded to changes in their environment to maintain an evolutionary advantage and we are now seeing real evidence of this adaptation as a result of hyperconnectivity. There are mixed feelings about whether these changes are a net positive or net negative to society, but few would deny that the change is happening, particularly amongst the younger generations.

2.3.1 Global Digital Landscape

Innovations in technology, particularly in digital media, increasingly are changing the way people use Media, Entertainment and Information (MEI) services. Nowadays people have many ways to interact and connect each other, with psychological consequences. The limit between private and professional lives is border line, and the possibility to catch real time information in every single moment are driving online connection time.

Since Tim Berners-Lee made the “World Wide Web” available to the public 25 years ago, the Internet has already become an integral part of everyday life for most

of the world's population. The time spend by people online is growing. Consider these approximate figures for 2017:

- 3,773 billion internet users;
- 2,789 billion active social media users;
- 4,917 billion mobile social accounts;

The main characteristics of today's consumption patterns can be summarized as follows:

- Mobile: the combination of faster mobile connection and improved access to smartphone has delivered the mobile's share of web traffic up to more than 50% and almost two thirds of the world population with a smartphone;
- Social and interactive: Social networking is the principal reason why people spend time online;
- Flexible and personalized: Users can have a more active role and more control over the digital media offerings they use and engage, compared with traditional media. Registration through website, giving personal information such as name, age, email etc. and cookies allow to personalize and fit content displayed based on each personality;
- More content: As content creation and distribution become simpler, a greater amount of content and services are becoming available;
- Collective: The possibility to connect, share recommend and communicate creates a collective experience that shapes not only behaviors and preferences, but also a collective consciousness of share beliefs, ideas and normal attitudes;
- Fragmented and multi-channel: The huge number of channels and creators makes content ever more fragmented;
- The higher the usage of digital media, the higher the willingness to pay: Increased connection and use of digital media should tip the revenue scale in industry's favour;

2.3.2 Internet of Things

The Internet of Things (IoT) enables objects (physical devices, vehicles, home appliances, buildings, etc.) sharing information and communicate with other

objects/members in the network, recognizing events and changes so to react autonomously in an appropriate manner (Morelli, 2013). The Internet of Things represents the next major economic and societal disruption enabled by the Internet, and any physical and virtual object can become connected to other objects and to the Internet, creating a fabric between things as well as between humans and things. The basic simplified work-flow of IoT can be described as follows:

- Object sensing, identification and communication of object specific information. The information is the sensed data about temperature, orientation, etc. based on the type of sensors used.
- Trigger an action. The received object information is processed by a smart device/system that then determines an automated action to be invoked;
- The smart device/system provide rich services and includes a mechanism to provide feedback to the administrator about the current system status and the results of actions invoked;

The IoT has enormous potentiality able to make such difference in economy and in the Internet itself, but it brings with itself different key challenges that must be face.

- Naming and identity management. The IoT will connect billions of objects in Internet, and each of them need to have a unique identity over the Internet. Thus, is necessary a naming and identity management system able to dynamically assign and manage unique identity;
- Interoperability and standardization. Many manufactures provide devices using their own technologies and services that may not be accessible by others. The standardization of IoT is very important to provide better interoperability for all objects and sensor devices;
- Information privacy. Since, every kind of daily use objects will carry different kind of object identification technologies and embed the object specific information, it is necessary to take proper privacy measures and prevent unauthorized access;
- Objects safety and security. The IoT consists of a very large number of perception objects that spread over some geographic are, it is necessary to prevent the

intruder's access to the objects that may cause physical damage to them or any change their operation (Brachmann, Garcia-Morcho, Keoh, Kumar, 2012);

- Data confidentiality and encryption. All the data transferred through different sensors and devices should be developed with security in mind, thus with an encryption mechanism.
- Network security. The data from sensors devices is sent over wired or wireless transmission network. The transmission system should be able to handle data from large number of sensor devices efficiently without loss data or external interference of any kind;
- Spectrum. The sensor devices will require dedicated spectrum to transmit data over the wireless medium. Due to limited spectrum availability, an efficient dynamic cognitive spectrum allocation mechanism is required to allow billions of sensors to communicate over the wireless medium;
- Greening of IoT. The network energy consumption is increasing at very high rate due to increase in data rates, increase in the number of Internet-enabled service and rapid growth of Internet connected edge-devices. The future IoT will cause significant increase in the network energy consumption. Thus, green technologies need to be adapted to make the work devices as energy efficient as possible;

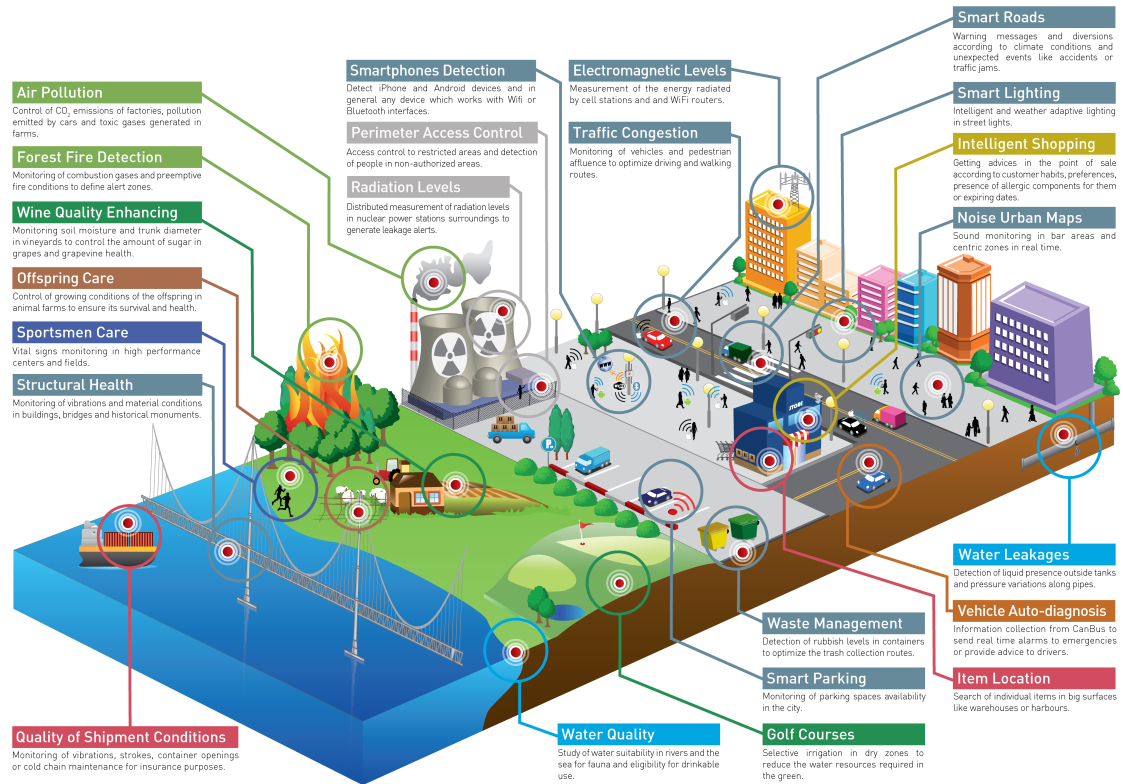


Figure 2.2: Sensors for Smart Cities, Internet of Things and Beyond.
Source: Libelium public domain, 2018.

2.3.3 Consumer Trust at Risk

The continuous innovation in digital media, and the rapid way it has changed business practices and user behaviour, created unprecedented opportunities for the media, entertainment and information (MEI) industry. But as these opportunities mature, consumer trust becomes ever more critical with fundamental concerns about truth, integrity and security are placing consumer trust at risk.

The barriers to content creation in digital media are today very low, thanks to innovation in this field. Today, anyone can create and publish content, and as consequence there is an increased quality control issue. The ease of creation has increased the risk of unethical online behaviour, with the posting and sharing of content designed to deceive, defame or misinform. The large amount of content available has made curating and distributing a much bigger challenge. Users themselves have become an important mechanism for distribution. Rather than rely

on the judgement of editors or decision-makers in the traditional media ecosystem, many users today choose to take more content from their social or professional networks. Given today's immense task of sifting through copious amounts of content in order to decide what to distribute, MEI distributors are turning to artificial intelligence and automation. Who play an important role here is the algorithms, strictly related to the consumer trust. This trust is at risk as evidence becomes available on how algorithms are structurally biased in the information they present to different users or are ineffective in screening out inaccurate content.

Because the digital media offers more content than can be reasonably consumed, much of it for free, a consumer's willingness to pay remains a key challenge for industry. Several studies on consumer readiness to pay for Facebook (in exchange for privacy or no advertising), for example, found little appetite for it. For Facebook, this is access and use of behavioural information for advertising purposes in exchange for free utilization of a robust social networking tool for the end user. But the idea of consumer reluctance to pay ignores the success of many digital media content providers. Consumers of digital media are willing to pay for products that fulfil their needs and offer good perceived value.

- Unique and high-quality content, such as that offered by HBO or The New York Times (NYT);
- Content that satisfies a burning need, such as Bloomberg's sale of business information to the trades, or demand in a niche market;
- A unique offering that fills a newly created need or gives consumers the flexibility to buy fragmented content, such as iTunes;

Today more users utilize advertising blocking in their devices. This represents a big challenge for the MEI industry. To do this could require the MEI industry to rely on advertising that respects user preferences for valued digital media, without the risk of misleading or exploiting the consumer. Exploitation can occur when advertising is based on behavioural data that the user did not consent to sharing. Or it can happen when transparency about the use of one's personal data is lacking, and the consumer is not offered appropriate benefits in exchange, such as free online services.

Consumer seems willing to pay for digital content when he/she thinks that value exchange between user and business is fair.

The cumulative use of digital media, from online buying, viewing, posting and sharing, reveals a huge amount about each user. Yet many users remain unaware that their increased digital engagement results in the accumulation of data from many disparate sources. These traces of personal data can be tagged, tracked, combined and analyzed, revealing more intimate information about users than previously imagined.

Security will be increasingly a major topic to address for MEI business in order to maintain consumer trust in the future. User fear data breaches which appear to be increasing in scale and frequency and they are also concerned about how their data are being used to market them.

Consumers seem reluctant to pay for privacy or control of data because they view them as already integral to the services they use, which is quite significant. Emerging digital users consider control over their data an inherent right for which they should not need to pay.

CHAPTER 3

WHAT WE NEED TO THINK ABOUT TODAY TO HELP SHAPE THE INTERNET OF TOMORROW?

What we need to think about today to help shape the Internet of tomorrow?

Until the mid-'60, openness and cooperation typified the software industry. Software was produced collectively, adhering to principles established in the field of academia. This collaborative process led to the birth of both the Internet and the Web.

The Internet is continuously changing and evolving, but the primary principle underlying the success of the Web is universality. Anyone can make a webpage, publishing any content that would linked through other websites, consulted from a completely different region or continent. The universal accessibility is under threat. Private companies, such as Facebook or LinkedIn do not want to share. They capture a huge amount of personal information, but they keep it to themselves. Similarly, Apple's iTunes store requires proprietary software to access it. You cannot access it from a browser, you cannot link to it and search engines cannot index it. This is a worrying trend. It goes against everything the Web stand for, everything that makes it the most widely adopted technology on the planet. As Tim Berners-Lee stated, "The decision to make the Web an open system was necessary for it to be universal. You cannot propose that something be a universal space and at the same time keep control of it."

The potential of the Web is based in its openness and security, thus also the decision regarding it, as its future, should be taken in a inclusive and democratic way. They key to the future is to put humanity at the center of the online world. Human values must drive technical development and use, we must have a public debate for society to agree on ethical standards and norms for the use of emerging technologies. These considerations should be applied in the design of every new technology developed, thus the industry should be proactive in incorporating independent ethical reviews into business decisions about emerging technologies.

Another key point is to apply human rights online as well as offline. Governments should not shutdown the Internet every time they need as a policy tool, because this is considered as limitations of human rights online. Individuals should continue to have the ability to communicate confidentially, anonymously and securely, so encryption should be encouraged as integrate feature of every new technology, because the users' interest and their own data should be protected. Application and service providers must be transparent about how and why they collect users' personal data. Encourage data minimization practices, insist on selective data collection and only for as long as necessary. Act now to close digital divides, prioritizing infrastructure development around the globe including high speed and wireless networks, community-based infrastructure and data centers. Providing youth and workers with the right skills for the new global economy. Incorporate security-by-design into devices and systems. Make the Internet economy work for everyone. Governments, institutions and industry must prioritize skills development and training to allow people to keep pace with innovation and its impact of jobs. Create an environment that incentive entrepreneurship such as new startups. Equal opportunity for everyone to benefit from the Internet economy. Governments in particular should provide tools and information in order to skill citizen about their privacy and online rights. Corporations should always respect user privacy and human rights, having direct responsibility if they do not do it. Openness, global reach and integrity must be the base for future network development

Technologist need to promote diversity in networks and services to allow for the next generation of products and services to emerge. Address the need for online social forms, thus making the Internet a safe place where everyone is free from online violence and harassment, without compromise free speech. Multistakeholder engagement is the way to develop norms of behavior. All stakeholders in society need to accept responsibility to ensure the openness of the Internet. Empower people to shape their own future. Stakeholder should support civil society and its critical role in protecting and promoting human rights online. Governments should support civil society's meaningful participation in domestic Internet policymaking.

CHAPTER 4

CROSSROADS IN THE INTERNET PATH

The world increasingly shaped by digital domain, we see an Internet that faces many challenges. We see an Internet at a crossroads, where we have critical choices to make about its evolution.

The Internet is described by its name, a short form of the compound word “inter-networking”. Its architecture is based into common protocols designed to connect any two networks which may be completely different in internal hardware, software, technical design and location. Its openness has enabled the Internet architecture to grow to a global scale. Silicon Valley and technology-dependent organizations would not survive without digital infrastructure: servers, programming languages, framework, and libraries. All of which are overwhelmingly based on free and open source code.

The Internet is transformative thanks to its openness. Its openness enables constant innovation and collaboration across borders. It is a radical concept, and nowadays it is constantly at risk. Governments block mobile apps or shut down the Internet at will, media trade groups lobby for expanded copyright worldwide and corporations seek to enclose and control whatever they can: email, messaging, social media, etc. The urgent question is, how can we preserve the open nature of the Internet, while at the same time building a digital world that is inclusive and welcoming at all?

The Internet belongs to us all, but a few large players dominate much of the online world. Without considering China, the Internet world is dominated by five companies, giants, from the United States. Precisely, these companies are: Amazon, Apple, Facebook, Microsoft and the end Alphabet, the parent company of Google. These companies have built technologies used and enjoyed by billions of us, but their consolidation of power, and business models that demand more and more information and data about us, could be a threat for the Internet and for the whole society?

Telecom companies also pose a threat to a decentralization when they offer sponsored deals on specific online content, like messaging or music, that puts smaller players at a disadvantage. The fight for net neutrality it is just started. How should we govern in a world where a handful of companies have more wealth than many nations? Can we distribute more control of Web technologies, using peer-to-peer, blockchain etc.?

Technological development is happening simultaneously in different contexts, including virtual reality, artificial intelligence, robotization, nanomaterials, and energy technology. All these developments have potentially significant social consequences, as digital platforms displace traditional companies, computers displace humans, and devices displace traditional channel of communication. Significant technological changes can shake up entire societies. While many of their consequence are beneficial, they can also lead to severe social tensions. The advent of the steam engine during the Industrial Revolution brought with it more efficient travelling and factories, but also pollution and later climate change. Rapid urbanization led to the appearance of both slums and creative cities, and while new jobs were created for millions of people, we were also left with new social problems, like unemployment and urban poverty. We can reflect this back to the technological developments of today.

Maybe not everyone knows it, but today we are sharing more personal information than ever before. Nowadays, the core business models of the Internet depend on knowing as much as possible about everyone, and analyzing, repackaging and selling that information. Data collection is accompanied by a constant risk of our social, financial, romantic, or political information being leaked in ways that expose us to harm. In 2017, the disclosures of breach after breach, for instance Equifax, Yahoo, Uber, etc., show that many of the companies we trust, giving them amount of data about us, are not doing enough. And of course, the prying eyes of governments are watching too, think about what Edward Snowden revealed about NSA surveillance program “PRISM”.

Security is only becoming harder to deliver at scale. Every technology, be it software or hardware, presents new risks. As the Internet expands with more

connected devices, the challenges will only grow. We have reached a point where you cannot opt out. When homes have listening machines, shopping centers have facial recognition camera, and satellite images can identify our cars, can we really control our digital footprints?

In a hyperconnected society, human beings, machines, and their surroundings are connected by millions of sensors. This fast-developing phenomenon includes the Internet of Things, connected devices and programmable world. Hyperconnected technologies develop fast, and also their interaction with us: they shape our lives, norms, values, and behavior. As a major global development of our time, the expansion of hyperconnected technologies has the potential to solve perhaps the greatest burning question faced by humanity: how to increase our wellbeing and capabilities without further burdening the planet. At the same time, hyperconnected technologies are shaping a world where single companies can wield enormous power over entire economies. Uber aims to become a global taxi monopoly, and Google and Facebook together control a staggering share of the flow of information. This is not just about the economy either: never before have single companies wielded so much power over our personal, social, and political lives.

Surveillance, by its nature, impacts on personal privacy. The issues of privacy and personal data protection have frequently been in the news in recent years, especially in the context of social networking, consumer profiling by online advertising companies, cloud computing and government surveillance. With the amount of data growing exponentially, there is little doubt that it will change the world in the coming years in ways that we can scarcely image today. Processing reliable data can help discover certain trends, which can contribute to reducing the waste of resource and improve policy-making. However, data can also be used to put people under complete surveillance, in breach of their fundamental rights. For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Is the society ready to tackle it?

4.1 Open vs. Closed

The debate has been going on ever since the Internet first started to hit the mainstream: the battle of open vs. closed, between the web giants and platforms, open web vs. closed garden, open source vs. proprietary standards. Being open is one of the basic principle of the web and the embodiment of much that is good about technology. Those who choose the opposite approach, however, argue that that some kind of central control is necessary, especially as our increasingly digital world gets more complex.

Think of the Internet history. Until the mid-'60, openness and cooperation typified the software industry. Software was produced collectively, adhering to principles established in the field of academia. This collaborative process led to the birth of both the Internet and the Web. By the '70s the software industry had developed beyond hardware manufacturers. Specialist companies were challenging the bundled hardware-and-software model. By the early '80s, led by Microsoft, charging a license fee for software became the norm. As the Internet matures, its initial decentralized form has been increasingly replaced by a small number of ad-financed centralized platforms, such as Facebook and Google. These platforms often design, control, influence, and “optimize” the user experience according to their own internal values and priorities, mainly through algorithmic filtering and computational inference of private traits from computational social science. The shift to a small number of controlling closed platforms stems from a variety of dynamics.

First of all, it is fundamental to define what do open and closed, related to Internet, mean. Defining a system “open”, means that it has to fulfill two rules:

- No restrictions are placed on participation in its development, commercialization or use;
- Any restrictions are reasonable and non-discriminatory, that is, they are applied uniformly to all potential platform participants;

Whereas, “closed” or “proprietary” system is where the carrier or service provider has control over applications, content, and media, and restricts convenient access to non-approved applications or content.

Take a look technically in some of the most used, closed and proprietary platforms, at business level. Nowadays in the information and technology sector, many firms implement business models relying on platform-mediated networks. Relevant companies such as Apple, Amazon, Google, Cisco, Microsoft, etc. have developed their own platform in order to engage with external stakeholder. A platform-mediated network is comprised of users whose transactions are subject to direct and/or indirect network effects, along with one or more intermediaries that facilitate users' transactions (Rochet and Tirole, 2003; Eisenmann, Parker and Van Alstyne, 2006; Evans and Schmalensee, 2007). The platform encompasses the set of components, such as hardware and software, and rules employed in common in most user transactions (Boudreau, 2008). Rules are used to coordinate network participants' activities (Baldwin and Clark, 2000). They include standards that ensure compatibility among different components, protocols that govern information exchange, policies that constrain user behavior, and contracts that specify terms of trade and the rights and responsibilities of network participants. Platform-mediated network encompass several distinct roles, including:

- Demand-side platform users, commonly called “end users”;
- Supply-side platform users, who offer complements employed by demand-side users in tandem with the core platform;
- Platform providers, that are first point of contact between user and the platform;
- Platform sponsors, who exercise property rights and are responsible for determining who may participate in a platform-mediated network and for developing its technology.

For every single platform, each of these roles may be open or closed.

For instance, a platform that has all four roles open is Linux. Anyone can use Linux (demand-side user role), any party can offer a Linux-compatible software application (supply-side user role). Any party can run the Linux operating system (OS) with server or personal computer hardware (platform provider role). Finally, being part of an open source community that maintains the OS kernel, anyone can improve it. Not like Linux, the Apple's iPhone in 2008 was closed with respect to three of the four roles, and is only open for some prospective demand-side users

under onerous terms. The only role that fulfilled the open standard was the demand-side user, because any organization or individual can use an iPhone. Other roles in the iPhone network are closed (Hagiu, 2006). Software application for the iPhone are only available through Apple's iTunes Store. Apple could reject third-party applications due to their vision, strategy or quality (supply-side user role). Only Apple manufactures and distributes the iPhone (platform provider role) and Apple is solely responsible for the iPhone's technology (platform sponsor role). Between Linux and Apple, there are platform that mix open and closed roles like Microsoft's Windows, that is closed at the sponsor level, but open with respect to other roles.

	Linux	Windows	Macintosh	iPhone
<i>Demand-Side User</i> (End User)	Open	Open	Open	Open
<i>Supply-Side User</i> (Application Developer)	Open	Open	Open	Closed
<i>Platform Provider</i> (Hardware/OS Bundle)	Open	Open	Closed	Closed
<i>Platform Sponsor</i> (Design & IP Rights Owner)	Open	Closed	Closed	Closed

Figure 3.3: Comparison of Openness by Role in Platform-Mediated Networks.
Source: Eisenmann, Parker, Alstyne, 2008. Harvard Business School

One problem with this fight, is that apps and walled gardens can be very appealing from a user-centric point of view (Lee and Mendelson, 2008). What many people do during a day could be check the email, probably in our Apple device, for instance an iPad, and that happen through an app: apple mail. During breakfast we probably browser Facebook, Twitter, and maybe The New York times, and here we are: three more apps. Make a Skype call and IM (instant messaging) conversations, more apps, and at the end of the day play some games on Xbox Live, and watch a movie on Netflix's streaming service: closed and proprietary platform. We have spent the day on the Internet, but not on the web. Over the past few years, one of the most important shifts in the digital world has been the move from the wide-open Web to semi closed platforms that use the Internet for transport but not the browser for display. It is driven primarily by the rise of the iPhone model of mobile computing. It

is the world that consumers are increasingly choosing, not because they are rejecting the idea of the Web but because these dedicated platforms often work better or fit better into their lives. After all, the Web is just one of many applications that exist on the Internet. Today the content we see in our browser accounts for less than a quarter of the traffic on the Internet, and it is shrinking. The applications that account for more of the Internet's traffic include peer-to-peer file transfers, email, company VPNs (Virtual Private Network), the machine-to-machine communications of APIs, Skype calls, online games, Xbox Live, iTunes, voice-over-IP phones, iChat, and Netflix movie streaming. Many new Net applications are closed, often proprietary, networks. People use the Net, but not the Web.

Who supports openness say their approach is best because allows creativity and a potential infinite number of people to contribute to a project. The concept of community always been part of the Internet, since day one, developing software and protocols completely open source and free. No gatekeepers, the Web is decentralized and anyone can start a web site. No one has the authority (in a democracy, anyway) to stop you from putting up a shingle. Neutrality, with possibility to reach any site. If it is on the web, you can find it and visit it. Sites on the web share common protocols and principles, and determine independently how work with each other. In contrast, defenders of the proprietary believe that the open model do not allows creativity, but maximizes error, less usability and lack of order. Freedom from centralized control results in an absence of standards, as well as a lack of discipline and accountability. Central control makes it easier to roll out features and keep a handle on errors, while proprietary standards allow developers to work faster and more efficiently, because they do not have to support multiple formats or guess where the next upgrade patch is going to come from.

Nowadays we have software like Linux, Firefox, PHP and Apache proves that, often, the best choice is open source, but it is not a one-way street. Some of the most successful companies in the world pursue a licensing model. Microsoft, Apple and Adobe among them. The story of industrial revolutions, after all, is a story of battles over control. A technology is invented, it spreads, and then someone finds a way to own it locking out others. It happens every time. Take railroads or telephones. The

invention of the switchboard was another open standard that allowed networks to interconnect. After telephone patents held by AT&T's parent company expired in 1894, more than 6,000 independent phone companies sprouted up. But by 1939, AT&T controlled nearly all of the US's long-distance lines and some four-fifths of its telephones. Now it is the Web's turn to face the pressure for profits and the walled gardens that bring them.

4.2 Centralized vs. Decentralized

Nowadays the Internet has become a necessity for modern living that it seems we cannot live without it. The Internet commercialization has led to its centralization that is controlled by the big players, but the original Internet was not like this.

At the beginning, the Internet was a project by the US Department of Defense to establish a computer data communications network that could withstand unforeseen events and disasters like war. If one part of the system fails, the rest can still function, this is reason must be decentralized. It must also able to communicate using peer to peer interconnectivity without relying on a single computer. Another important consideration is that the computers must be able to share among different systems, in order to be part of a network. It all started with ARPANET in October 29, 1969, but the concept of decentralized network came to footlights through the Napster case. Napster was a music sharing application, originally release in 1999, which granted users access to an enormous database of file through P2P system (peer-to-peer), but it was shot down in July 2001 due to copyright indictments. It was the end of Napster but it was not the end of P2P. Open-source developers set about creating a second generation of P2P software products without the central indexing function that had been Napster's downfall: BiTorrent, Bitcoin, I2P, etc. Theoretically, the Internet is still decentralized. No one own all or a considerable portion of the network or infrastructure that connects that world wide web. But over the years, companies such as Facebook and Google have come to dominate the services that support the Internet. Users online spend much part of their time through their services, giving them huge amount of data. This happens also thank to innovative ideas able to provide easy-to-use and efficient platforms for users to communicate, publish and discover content,

which encouraged more users to sign up for their services. This huge amount of power has turned these companies into gatekeepers of information, making the Internet more centralized.

Centralized Internet means that there is a mandatory centralized point (hardware) through which all the data on the network must pass. It is mostly a server as in client-server model bank use, or a hub, which is what most social media site and web hosting sites use. Put another way, in a centralized internet model, all of our data has to run through companies, which makes accessing our data easier and faster. However, that ease come at a cost. Because so much data is running through these centralized locations, it is easier for an outside person, company, or government to view that personal information, whether you want them to or not. The decentralized Internet can be identified using peer to peer (P2P) connections rather than using a single point network access. Peer-to-peer networks consists of devices (web server or end user computers) that participate on equal terms in a type of communication. Each peer can communicate with other peers and there is no distinction between consumers or producers, clients and servers, etc. It is simply many devices communicating with many devices. The most important difference between centralized and decentralized Internet is that the latter connects to different points (peers: other computers, servers etc.) without having to go through a mandatory point.

Nowadays social media platforms such as Facebook dictate what news their users should read. Facebook now has more than 2 billion monthly active users. Another big player is Google, the undisputed ruler of web search, which processes more than 5 billion queries per day. This huge amount of power has turned these companies into gatekeepers of information, with the consequence that we have to trust them, without having any certainty. Another possible issue with current centralized systems is that they run on centralized architectures. Every internet company has its own data centers, where it stores user data and runs its applications. One of the major problem of centralized architectures, is that they suffer from single points of failure. When the servers of centralized services such as Amazon Web Services fail, all the website and applications that depend on them stop working. Centralized architectures are also vulnerable to Denial of Service and Distributed Denial of Service (DoS/DDoS)

attacks, because they provide attacker with a single target to hit. Centralized architectures also give rise to serious privacy concerns. Users have little or no idea about that goes on behind the walled gardens of centralized services. Therefore, they do not precisely know how much data these services collect about them and they what they use them for. There is also issue of who these services share their user data with. All major internet companies have record of giving away user information to government agencies without acquiring their consent, or selling them to third parties. More precisely, the problem is that users do not own their own data and they surrender it to the applications and services they use. They are only generating data for the profit of the services they are using, and they earn no share of the revenue.

P2P is not a new technology, it has been there for a long time. On the Internet, peer-to-peer applications use peer-to-peer protocols that are based on the IP-protocol. Peer-peer networks have a series of particular advantages:

- They have no single point of failure because there are not centralized entities;
- They can grow easily because each additional participant adds extra resources (traffic capacity, storage, computing power) to the network;
- There is no administration because there is no central authority;
- Faults have minimal impact because there are no centralized resources and there a naturally high level of duplication of resources;
- They grant freedom to their users. Not only are the participating devices equals, the participating users are also on equal footing.

One of the important tasks of a peer-to-peer application is to organize the network an locate resources in the network. The decentralized internet model improve the possibility for care about our online privacy as well as a return to how the web was originally created. Rather than relying on centralized servers of hubs to store data, a decentralized web relies on peer-to-peer connections. Not everyone uses their data storage, bandwidth, and processing power at the same time. Instead of relying on companies to store our data, this version of the web would break down our data into microscopic chunks and scatter it among other people's unused storage spaces.

It all comes down to one argument: privacy vs. convenience. As the web exists in its current state, a shocking amount of online communications flow through a handful

of corporations. This centralization means that companies such as Google and Amazon always have our data ready to share with us immediately, but there are also risks. Because this huge amount of data are stored on these cloud-computing software, potentially target for hackers. When we use a service such as Facebook or Uber, we agree to a term of service. Most people do not waste their time on the legalese, but many of these agreements give companies the right to look through our information and sell it to other companies. There is a lot of money to be made in selling our information, and not too much profit in protecting it. The decentralized Internet is still alive, and through the P2P protocol still many models are growing up and shaking up different sector such as the financial industry through Bitcoin and peer-to-peer currency.

4.3 Artificial Intelligence vs. Human Intelligence

We are in the midst of a revolution in machine intelligence that will affect every aspect of the human society. The opportunities of this revolution will create are immense, ranging from new services and breakthroughs to the augmentation of human intelligence. There are considerable uncertainties about machine intelligence, including the delegation of decision-making to machines, lack of transparency and whether technological change will outpace the development of governance and policy norms. Automation may deeply shape industry, with consequences for employment. Governments and societies have to be ready for these changes.

The field of artificial intelligence was not formally established until 1956. In 1956, a conference “Artificial Intelligence” was held for the first time in Hanover, at Dartmouth College. Although the term was not coined until 1956, the roots of the field go back to at least the 1940s (McCulloch and Pitts, 1943), and the idea of AI was crystalized in Alan Turing’s famous 1950 paper, “Computing Machinery and Intelligence.” Turing’s paper posed the question: “Can machines think?” The famous Touring test was based on that question, and raised the possibility that a machine might be programmed to learn from experience much as a young child does. In the ensuing decades, the field of AI went through ups and downs. It wasn’t until the late 1990s that research progress in AI began to accelerate, focusing on the application of

AI to real-world problems, such as in medicine. In 1997 had great public impact the victory of IBM's chess-playing computer Deep Blue over world champion Garry Kasparov. Other significant breakthroughs included DARPA's Cognitive Agent that Learns and Organized (CALO); IBM's question-answering computer Watson's victory in the TV game show "Jeopardy!"; and the surprising success of self-driving cars in the DARPA Grand Challenge competitions in the 2000s. The deep attention on AI began around 2010, driven by three factors: the availability of big data, the growing amount of data and information thanks to big data, and always more powerful computers. The improvements made in this period was important. The new wave of artificial intelligence is based on insights derived from the way animals and people learn and analysis of the underlying brain circuits that allowed theorists to develop supervised learning and algorithms. The AI ability to replicate specifying human tasks will permeate society. Siri by Apple is on the beginning, driverless cars and trucks will become the norm.

The Artificial Intelligence practitioners do not universally accept a single definition of AI. The diversity of AI problems and solutions, and the foundation of AI in human evaluation of the performance and accuracy of algorithms, makes it difficult to clearly define a bright-line distinction between what constitutes AI and what does not. We can argue that Artificial Intelligence can be defined as a science and a set of computational technologies that are inspired by the ways people use their nervous systems and bodies to sense, learn, reason, and take action (Nilsson, 2010). On the other hand, Human Intelligence is defined as the intellectual prowess of humans, which is marked by complex cognitive feats and high levels of motivation and self-awareness. Through their intelligence, humans possess the cognitive abilities to learn, form concepts, apply logic, comprehend ideas, retain information, and use language to communicate.

Artificial Intelligence is already changing our daily lives, almost entirely in ways that improve human health, safety, and productivity. AI technologies have greater potential to make driving safer, help children learn, and extend and enhance people's lives. In fact, beneficial AI applications in schools, homes, and hospitals are already growing at an accelerated pace (Crawford, 2016). Major research universities devote

departments to AI studies, and technology companies such as Apple or Facebook spend huge resources regarding AI applications.

Innovations relying on computer-based vision, speech recognition, and Natural Language Processing have driven these changes, as have concurrent scientific and technological advances in related fields. AI is also changing how people interact with technology. People's future relationships with machines will become more personalized as AI systems learn to adapt to individual characteristics.

We can summarize eight domains where AI is already having or is projected to have the greatest impact: healthcare, education, transportation, low-resource communities, employment and workplace, public safety and security, home/service robots, and entertainment. Each domain faces varied AI-related challenges, including the difficulty of creating safe and reliable hardware for sensing and effecting (transportation and service robots), the difficulty of smoothly interacting with human experts (healthcare and education), the challenge of overcoming fears of marginalizing humans (employment and workplace), and the risk of diminishing interpersonal interaction (entertainment).

In each domain, even as AI continues to deliver important benefits, it also raises important ethical and social issues, including privacy concerns. How the difference between man and machine might affect the trust, or lack of, in the digital domain, how it may affect surveillance and when machines are appropriate in these contexts? AI will be able to collect a huge amount of data, thus positioning itself in the business of Big Data. Several crucial surveillance trends have in fact been the result of increasing data creation and analysis possibilities directly related to Big Data (Lyon, 2014). With the incorporation of intelligence machines, we can introduce people's personal privacy even cheaper and faster. This seems to be a general concern, but it might be a bit misplaced. What is argued is that one of the major concerns are regarding informed consent (Flyverbom, 2015). That we are agreeing to various aspects around our privacy that we are actually not aware of. The Internet in its foundation was established as an optimization of information exchange, but in the process of the development of it, we forgot to think about control, power and privacy (Bostrom, 2015). So now we are unaware of who can see what we do and how it can

be used. Living online is an exchange, between getting very useful tools for free, and giving up all our data in the process (Hardt, 2016). The data we are generating online is in fact persisting under the control of other, so you need to ask yourself, do you trust those actors in power?

The research that fuels the AI revolution has also seen rapid changes. The main are the maturation of machine learning, stimulated in part by the rise of the digital economy, which both provides and leverages large amount of data. Another factor is the rise of cloud computing resources. New platforms and markets for data-driven products, and the economics incentives to find new products and markets, have also stimulated research advances. These trends drive the AI research into both fundamental methods and applications areas. Large-scale machine learning concerns the design of learning algorithms, as well as scaling existing algorithms, to work with extremely large data sets. Deep learning, a class of learning procedures, has facilitated object recognition in images, video labeling, and activity recognition, and is making significant inroads into other areas of perception such as audio, speech, and natural language processing. Reinforcement learning is a framework that shifts the focus of machine learning from pattern recognition to experience-driven sequential decision-making. Robotics is currently concerned with how to train a robot to interact with the world around it in generalizable and predictable ways, how to facilitate manipulation of objects in interactive environments, and how to interact with people. Computer vision, and for the first time computers will be able to perform some vision tasks better than people. Natural Language Processing is quickly becoming a commodity for widely spoken language with large data sets. Collaborative systems research models and algorithms to develop autonomous systems that can work collaboratively with other systems and with humans. Crowdsourcing and human computation research investigates methods to augment computer systems by making automated calls to human expertise to solve problems that computers alone cannot solve well. Algorithmic game theory and computational social choice, mean how system can handle potentially misaligned incentives, including self-interested human participants of firms and the automated AI-based agents representing them. Internet of Things (IoT) research is devoted to the idea that a wide array of devices, including

appliances, vehicles, buildings, and camera can be interconnected to collect and share their abundant sensory information to use for intelligent purposes. Neuromorphic computing is a set of technologies that seek to mimic biological neural networks to improve the hardware efficiency and robustness of computing systems.

Artificial Intelligence and machine learning are surely becoming part of our lives and the predicted changes in real life will be drastic. Of course, this will also affect the digital space, maybe even more so, transforming major parts of the Internet as we know it today. Considering all these aspects, AI regulation is essential, but a regulation able to understand the potential of AI, but with respect of human rights. AI has the potential to be used for good or nefarious purposes, it depends in how it will be used.

4.4 Freedom vs Control

Since so much of life has moved online, a clash has merged between the opposing values of Internet freedom, and Internet control. Should the Internet be free from authority interference? Too much freedom on Internet could bring too many risk?

The Internet is and has always been a space where participants battle for control. The two core protocols that define the Internet - TCP and IP – are both designed to allow separate networks to connect to each other easily, so that networks that differ not only in hardware implementation but also in their politics of control (consumer vs. research. vs. military networks) can interoperate easily. Initially mechanisms of Internet control were largely developed by members of the Internet community in the form of norms enforced with little or no intervention of courts or law enforcement. Members of the Internet community, especially its technical administrators, enforced these norms by threatening temporary or permanent disconnection from the Internet. By avoiding government interference, the ambition was to achieve freedom of speech and freedom from prejudice. These goals were represented in John Perry Barlow's "Declaration of the Independence of Cyberspace", where he evokes the US Declaration of Independence, particularly the right of free speech. He described the Internet as borderless, stateless world where anyone, anywhere should be able to express his or her beliefs without fear of censorship. Increasingly however, Internet

control mechanisms – including technical, legal political, and social tools – have been imposed by governments due to a perception that self-regulation is no longer sufficient to deal with challenges increasingly posed by the Internet. Those challenges include the rapidly growing number and diversity of users, intensifying criminal activity, the role of the Internet as a core social infrastructure, and the diversity of political philosophies of participating countries.

A free and open Internet has become a source of innovation, social interactions and a platform for free expression. However, the democratization of information by the world-wide-web depends on factors as access, and can perhaps be compromised by online filter bubbles, in the end resulting in a misinformed and misguided public. The democratization of information depends on digital media that are free from government control and big business forces. But this freedom, in a post 9/11 world, has become a murky business of security and online content control issues. The internet control mechanisms are complex set of check and balances, spread between governments, companies, international bodies and individuals has evolved over time and is continuously in flux. The Internet empowers individuals and serves innovation, education, civil rights and community development through individual freedoms of expression online. However, with increased ease of communication provided by the Internet have come increased efforts by government to police online content. While government surveillance of internet activity in order to protect national security, combat terrorism, protect copyrighted material and minimize highly offensive content including child pornography seem justifiable, it may be difficult to draw the line between internet surveillance that only targets these areas and surveillance that violates constitutional rights.

The Internet should be protected from government censorship just as much as any other traditional communications medium has been. Should be taken an approach to the internet freedom/control issue based upon tradition of liberalism, in which individual rights and freedoms should be protected at all costs. With respect to internet regulation and surveillance, these rights include individual rights to privacy, due process, freedom of expression and freedom of information.

4.5 Spirituality vs. Hyperconnectivity

Nowadays the time we spend only is exponentially increase. Technology gives us many advances, such as be more effective in our work, allowed us to connect with friends, family and colleagues across the world. However, often with rapid change, there is a cost. And far too often, face-to-face interactions are suffering because of the effects of technology and how it dominates our world. Whatever our position on technology, the simple facts are, we cannot avoid it. Technology is part of our daily life, from the moment we wake up until we go to sleep at night.

The result of this increasingly accelerated communications evolution is that today we are faced with the phenomenon of hyperconnectivity, a term coined by scientists studying person-to-person and person-to-machine communication in networked organizations, referring to use of multiple means of communication, such as email, instant messaging, phone. Hyperconnectivity has usually been celebrated as a sign that people are able to remain more connected with each other than ever before; but in truth, the whole picture may be considerably more complicated than that. For institutions and organizations, it is driving monumental shifts in terms of impact on their work styles, functions, and missions in a variety of realms. Urbanization is one these realms, in which hyperconnectivity offers some obvious benefits such as improved standards of living in remote areas cause the result of increased availability of technology and better access to government services, education, and healthcare could substantially improve the quality of life for many. On the political front, it enables governments to improve communication with their citizens by sharing information more quickly and transparently, and it has the potential to restructure this relationship. In recent years, in the education sector, there has been a proliferation of online learning opportunities, who reflects the ability of technology to support anytime and anywhere connections, as well as individualized learning plans. As broadband connectivity become more ubiquitous, the use of virtual education tools to reach populations in remote areas becomes much more flexible. In the realm of healthcare, hyperconnectivity is already proving to have huge potential. Machine-to-machine-to-human (M2M2H) communications solutions – which are becoming a reality today – can improve patient care, support mobile and virtual care, and reduce

travel requirements for both patients and physicians. With a hyperconnected healthcare sector, doctors and nurses can remotely monitor and diagnose patients continuously via medical application. Hyperconnectivity is affecting enterprises of all sizes and types. In the real sector, hyperconnectivity is already a pervasive force in the interaction between buyers and sellers. The next stage in this transformation is in the area of logistics – where the Internet of Things and related hyperconnectivity will transform the supply chain and connect customers, suppliers, manufacturers, and retailers with each other in a more efficient process (Ferreira, 2011). Another key concern will be its interactions with customers and customer relations management, considering that today the process of interacting with them is migrating to the digital world and to be truly focused to customers complaints, companies must learn how to better manage relationships with their relationships with their customers in the hyperconnected world.

The technology opens up possibilities for communication that were almost literally unthinkable prior to its advent. It is now possible to keep in touch with friends and family, no matter how far one moves away from them, get more and better information through websites, search engines and social media in every moment, support the development of what has been termed the Internet of Things that embrace a broader meaning of communication, machine-to-machine and people-to-machine. Hyperconnectivity ensures that everyone can offer input on just about everything and through service records, virtually unlimited storage capacities, miniaturized video camera ensures that a large portion of everyone's daily activities and communications are part of a semi-permanent record. The cumulative effect of hyperconnectivity is that the limitations of time and space have largely been overcome. Experience is virtualized. You no longer need to be in the same room, or even the same country, as your colleague, your teacher, or your doctor (Moe, 2015). It can be a powerful tool for collaboration that drives global alignment, increased efficiency, and material development, but it could involve many other risks. We are entering the age of hyperconnectivity, with significant possibilities but also risks. It empowers corporates and governments to surveil users (attendant loss of privacy and security), improve Artificial Intelligence a such level that could displace of labor, and

the addictive technologies that have captured the attention the youngest generation. About this concept, the long-term effects on children growing up with screen time are not well understood but early signs are not encouraging: poor attention spans, anxiety, depression and lack face-to-face conversations and connections are some of the correlations already seen, as well as the small number of teens who become addicts and non-functioning adults (Subrahmanyam, Kavery, Greenfield, 2008). Engaging apps and digital experiences are addictive and there has been little progress in creating a healthy consumption model for digital experiences, thus people's well-being will continue to be affected by the Internet because there are products and services built to do exactly this. We already seen some negative effects. Digital communications and the time they take away from personal interaction are contributing to growing isolation, less ability to focus, more ability to be deceived by bad actors (fake news).

Real word interaction allows us to understand each other profoundly and allows us to get to know each other down to the most fundamental parts of who we are. Social media and social connections just do not have the same level of profound connectedness. We are in fact becoming more "connected" through social media in the very sense of the word, but this "connection" is one that we do not want to replace our real life connections with. Social media can truly have harmful effects on us psychologically if we use it to replace rather than enhance and if we do not realize that the connections we are establishing through these mediums are not suffice for our social development.

4.6 Privacy vs. Surveillance

The issues of privacy and surveillance have frequently been in the news in recent years, especially in the context of social networking, national security, consumer profiling by online advertising companies and cloud computing. Privacy and security are not contradictory priorities that need to be balanced. Security is a key element of our privacy and freedom. If security is being balanced against freedom, it is no longer fulfilling its role. These topics need to be asked now because of the radical increase in surveillance during the last decade, as the revelations in 2013 made possible by NSA-

whistleblower Edward Snowden on the reach of global surveillance practices have asked a fundamental examination of the role of intelligence services in conducting coordinated cross-border surveillance.

Beginning in 1946, an alliance of five countries composed by the US, the UK, Australia, Canada and New Zealand, developed a series of bilateral agreements over more than a decade that became known as the UKUSA agreement (Aldrich, 2004). This established the “Five Eyes” alliance for the purpose of sharing intelligence, but primarily signals intelligence derived from electronic signals and systems such as radars, communication systems, and weapon systems (Lander, 2007). The close relationship between the five states is evidenced by documents released by Snowden in 2013. The Five Eyes agencies have found ways to infiltrate all aspects of modern communications networks: forcing companies to give them their customers’ data, and tapping fiber optics cables between the same companies’ data center anyway; accessing sensitive financial data through SWIFT, the world’s financial messaging system; spending years negotiating an international agreement to regulate access to the data through a democratic and accountable process, and then hacking the networks to get direct access; threatening politicians with trumped-up threats of impending cyber war while conducting intrusion operations that weaken the security of networks globally; and sabotaging encryption standards and standards bodies, thereby undermining the ability of internet users to secure information (MacAskill, 2013)

The discussion about privacy and surveillance has to start from their definition. Privacy, generally, is a state in which one is not observed or disturbed by other people, the state of being free by public attention. At the internet level, is the privacy and security of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. Against the concept of privacy, is needed to explain what really mean surveillance. Surveillance is the monitoring of behavior, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people, while related to Internet is the monitoring of computer activity in a network, online activities, objects or processes that are

operated from or on the network (La Rue, 2013). However, at times it is perceived as a threat to network users as an invasion of privacy.

The world has changed since the 1940s. Now, private documents are stored in unknown data centers around the world, international communications are conducted daily, and our lives are lived online. This shift in communications infrastructure means that communications travel through many more countries, are stored in a variety of countries, particularly through the growing popularity of cloud computing and are thus vulnerable to interception by multiple subjects. One of these subjects are Governments, specifically their national intelligence agencies. Surveillance has many times been cited as necessary to fight terrorism, to prevent crime and social unrest, to protect national security, and to control the population. In modern society, the deliberation around privacy related to surveillance is a debate about modern freedoms. As we consider how we establish and protect the boundaries around the individual, and the ability of the individual to have a say in what happens to him or her, we are equally trying to decide: the ethics of modern life, the rules governing the conduct of commerce, and the restraints we place upon the power of the state. Technology has always been intertwined with this right. Today our capabilities to protect privacy is much better respect the past, yet the capabilities that now exist for surveillance are without precedent. We can now uniquely identify individuals amidst mass data sets and streams, and equally make decisions about people based on broad swathes of data. It is now possible for companies and governments to monitor every conversation we conduct, each commercial transaction we undertake, and every location we visit. These capabilities may have negative consequences on individuals, groups and even society as it chills action, excludes, and discriminates.

The way the global communications infrastructure is built requires that the right to privacy of communications be exercised globally. Privacy is necessary for an open society in the electronic age, and since we desire it, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for transaction, therefore we all need anonymous transaction systems and cryptography to ensure that.

CHAPTER 5

HOW WILL INTERNET EVOLVE?

So far, the story of the Internet has followed the same tragic narrative that is happen other information technologies: the telegram, telephone, cinema, radio, and television. Each of these had roughly the same story:

- Inventors discovered the technology;
- Hobbyists pioneered the applications of that technology, and popularized it;
- Corporations commercialized the technology, refined it, and scaled it;
- Once the corporations were powerful enough, they tricked the government into helping them lock the technology down “natural monopolies”;

After a long period of stagnation, a new technology emerged to disrupt the old one. This loop has repeated itself so many times that it takes the name of “The Cycle” (Wu, 2013). “Tim Wu (2013)” refers that history shows a typical progression of information technologies, from somebody’s hobby to somebody’s industry; from jury-rigged contraption to slick production marvel; from a freely accessible channel to one strictly controlled by a single corporation or cartel – from open to closed system.

Right now, we are in step four in the open internet’s narrative, surrounded by monopolies, and there is not step five in sight. The Internet is the ultimate information technology capable of supplanting the telegram, telephone, radio, cinema, television, and much more, and there is no clear way to disrupt it. There are many players on this global chess board: governments, telecom monopolies, internet’s company giants, hackers, and final consumer. The war for the open or closed internet is the defining issue of our time.

5.1 Walled Garden

In the mid-1990s, the Internet underwent a dramatic shift away from research-oriented uses by a small professional community, to a mainstream platform whose technical underpinnings were privatized, and whose resources became dominated by

commercial interests. This change prompted the development of walled gardens (closed or exclusive information services, content or media on platforms) typified by AOL, whose early objective was to steer subscribers away from the open internet to the company's proprietary services, and followed by Yahoo in the late 90s. But Yahoo was a candle in the sun compared to the ultimate walled garden, such as Facebook.

Nowadays something important has changed in the way mainstream consumers use the Internet, as well electronic and computing devices. Today the content users see in their browsers account for less than a quarter of the traffic on the Internet. The applications that account for more of the Internet's traffic include peer-to-peer file transfers, email, company VPNs, the machine-to-machine communications of APIs, Skype calls, voice-over-ip phones, and Netflix movie streaming. Many of the newer Net applications are closed, often proprietary networks (Anderson and Wolfe, 2010). Take a look on Facebook, for instance. For many younger internet users in particular, Facebook for effectively is the Internet, because it gives them everything they needs: games, social contact, some information, phot browsing etc. They use apps on their phone for virtually everything, and barely ever use a browser. Facebook's organization of information and relationship became, in a remarkably short period of time, a redoubt from the Web, a simpler more habit-forming place. Developers create games and applications specifically for use on Facebook, turning the site into a full-fledge platform. In terms of registration numbers or sheer time spent, Facebook became a parallel world to the Web, an experience that was vastly different and arguably more fulfilling and compelling and that consumed the time previously spent idly drifting from site to site.

Since the beginning of this decade, the Internet has become dominated by big powerful walled gardens and ecosystems as explained before: Facebook, Amazon, Netflix, Apple, Microsoft and Alphabet. Beside these giants, there is another huge threat for the openness of the Internet: the Internet Service Providers (ISPs) (see chapter 2.1.1.). These ISPs control millions of miles of copper cables that they buried in the ground back in the past, and satellites they shot up into orbit. They constantly break the law, tie up regulators in lengthy court battles, and make it practically

impossible for anyone, even to enter their markets. The ISPs do all this for one reason and one reason alone: in this way they can avoid free market competition. For the past years, the public had a weapon against these ISPs, it is called Net Neutrality. Net neutrality is a term coined by Columbia University media law professor Tim Wu in 2003, who define it as the principle that internet service providers treat all the data on the internet equally, and not discriminate or change differently by user, content, website, platform, application, or method of communication (Wu, 2003). The ISPs do not make nearly as much selling you a data plan as they used to make selling you cable plan, though. Their goal would be to lock down the internet into “channels” or packages for particular data services and then forcing you to buy one of those.

+ Smart Net
Oferta da 1ª mensalidade de uma Smart Net com 10GB/mês adicionais ⁽¹⁾

MESSAGING	SOCIAL	VIDEO
		
€4,99/mês €6,99/mês 1 mês grátis Aderir	€4,99/mês €6,99/mês 1 mês grátis Aderir	€4,99/mês €6,99/mês 1 mês grátis Aderir
MUSIC	EMAIL&CLOUD	MEO
		
€4,99/mês €6,99/mês 1 mês grátis Aderir	€4,99/mês €6,99/mês 1 mês grátis Aderir	Tráfego grátis para apps MEO já incluído no seu tarifário

Figure 4.4: Portuguese Internet Service Provider MEO Offers for Smartphone Contract. Source: MEO public domain.

In a post-net neutrality world, there is a fear that startups and small companies will not be able to compete with big companies. There is a fear the ISPs will be able

to censor competitive content or degrade our ability to consume it if we do not pay more. There is a fear the ISPs could package the Internet into bundles like cable TV (movie site, social media site, blogs, etc.). There is a fear that privacy is over forever. The web of countless entrepreneurs was being overshadowed by the single entrepreneur mogul visionary model, a ruthless paragon of everything the Web was not: rigid standards, high design, centralized control. We are slowly but surely creating an Internet that is abandoning its original values.

5.2 Open Bush

The Internet is the ultimate information technology capable of supplanting the telegram, telephone, radio, cinema, television, and much more, but there are many players on this global chess board. Governments, telecom monopolies, internet giants like Google and Facebook, NGOs, think tanks, startups, hackers and civil citizens. The war for the open internet is the defining issue of our time.

What does it mean open bush? Open bush means chaos, that would be the only word capable to describe the open internet. The open internet is distributed. It is owned in part by everyone and in whole by no one. It exists largely outside of the boundaries of governments, and it is this way by design. This reflects the wisdom of Vint Cerf, Bob Khan, J. C. R. Licklider, and all who pioneered the internet. The open internet is a where anyone can publish content, and anyone can then consume that content.

Our modern society, everything from hospitals to stock markets, runs on software. Nearly all software today relies on open source code, mean many times free and always public, written and maintained by communities of developers and other talent. Open source code can be used by anyone, from companies to individuals, to build software. This type of code makes up the digital infrastructure of our society today. The primary principle underlying the success of the Internet and the web is openness and universality. Anyone can make a webpage, any content can be put on a webpage, any webpage can link to any other, a webpage can be viewed at any screen size and any connection speed from any device connected to the internet. Anybody can access the Web from anywhere. This universal accessibility is under threat. Facebook,

LinkedIn and other web giants do not want to share. They capture a huge amount of personal information, such as your name, age, gender locations, etc., but they keep it to themselves. Similarly, Apple's iTunes store requires proprietary software to access it. You cannot access it from a browser, you cannot access it from a browser, you cannot link to it and search engines cannot index it. This trend goes against everything the Web stands for, everything that makes it the most widely adopted technology on the planet.

As Tim Berners-Lee stated, "The decision to make the Web an open system was necessary for it to be universal. You can't propose that something be a universal space and at the same time keep control of it".

CHAPTER 6

CONCLUSIONS

This dissertation is focused on Internet since its fundamental relation and influences with management topic. Nowadays Internet is the crucial point where technologies innovations are developed, everything is based on it. Take in consideration IoT, is shaping many aspects in management, from logistics to production. Considering this influence, it is important to understand how Internet will evolves, and in order to do that should be analyzed many aspects: from the initial architecture through Internet was created to nowadays governance. The present Internet design is taking part within organizations that have historically focused more on engineering than innovative vision and social interactions, but the growth brings the system to a new environment that the original designers may not have envisioned, together with new requirements that must be met. Through two case studies has been possible to have a clear picture of what is the actual status of Internet, and most importantly, what are the issues that must be tackled in the Internet and technology domain.

What has been asserted throughout this dissertation, is that the Internet is in front of six crossroads in its path, and choose one direction respect the other will have deep consequences in every sector, management included. The six crossroads are:

- Open vs Closed;
- Centralized vs Decentralized;
- Artificial Intelligence vs Human Intelligence;
- Spirituality vs Hyperconnectivity;
- Privacy vs Surveillance.

Right now, we are approaching the end of the 3rd industrial revolution and entering into the 4th that is pushed forward by the “internet of everything” and Artificial Intelligence. But let’s look back to the time of the 1st industrial revolution where we saw unprecedented economic growth. The technology in question was the steam engine and other machineries to automate the textile manufacturing. Today, instead of steam engine we have Internet. Understanding how it evolves will have enormous importance. Internet

in the next ten years will change, and with him all the sectors that nowadays use this technology. Through this dissertation I want show an overview of what will be the future decisions regarding Internet in order to understand how will impact management topic, developing two different scenarios, based on open or closed paradigms.

What is come to light is that technology access will makes increasingly more difference and the main technology driver for the 4th industrial revolution is the trusted connectivity through Open Internet and the skill of the people. These are the drivers for the future networked society.

BIBLIOGRAPHY

- Anke, J. & Sundaram, D. 2006. *Personalization techniques and their application*. Hershey, USA: Idea group reference.
- Baran, P. 1964. *On distributed communication. Introduction to distributed communications networks*. Santa Monica, California: The Rand Corporation.
- Beder, S. 2006. *Suited themselves: how corporations drive the global agenda*. London: Earthscan.
- Blazic, J. B. 2011. Four scenarios for future evolution of the Internet. *Ieee technology and society magazine*. Winter 2011: 39-46.
- Blazic, J. B. 2010. *The future of the Internet: tussles and challenges in the evolution path as identified by EIFFEL think tank*. 2010 fourth international conference on digital society.
- Berners-Lee, T. 2000. *Weaving the web: the original design and ultimate destiny of the world wide web*. New York: Harper Collins
- Bessant, J., & Tidd, J. 2013. *Managing innovation*. West Sussex: John Wiley & Sons Inc.
- Boucher, S. 2004. *Europe and its think tanks: a promise to be fulfilled*. Studies and research n°35, Notre Europe, Paris.
- Brousseau, E., & Marzouki, M., & Méadel, C. 2012. *Governance, regulations and powers on the Internet*. Cambridge: Cambridge University Press.
- Buzan, B., & Lawson, G. 2015. *The global transformation: history, modernity and the making of international relations*. Cambridge: University of Cambridge Press.
- Cailliau, R., & Gillies, J. 2000. *How the web was born*. Oxford: Oxford University Press.
- Castells, M. 1989. *The informational city: Information technology, economics restructuring, and the urban-regional process*. Oxford: Blackwell Publishers.
- Castells, M. 2010. *The information age: Economy, society, and culture*. West Sussex: John Wiley and Sons.
- Castells, M. 2002. *The internet galaxy: Reflections on the internet, business and society*. Oxford: Oxford University Press.

- Castells, M. 2005. *The network society: From knowledge to policy*. Washington, DC: Brookings Institution Press.
- Costa, C. M. 2016. Think tanks num mundo globalizado. In Mira, M. R. (Eds.), *A comunicação mundializada*: 110-111. Lisboa: Cooperativa de Ensino Universitário-CRL.
- Cheok, A. D. 2017. *Hyperconnectivity*. London: Springer.
- Chesbrough, H., W. 2003. *Open innovation*. Boston: Harvard Business School Press.
- Christiansen T. & Piattoni S. 2004. Informal Governance in the European Union: An Introduction. In S. Piattoni & Christiansen T. (Eds.), *Informal Governance in the European Union*: 1-21. Cheltenham: Edward Elgar Publishing.
- Domingue, J., & Galis, A., & Gavras, A. 2011. *The future Internet. Future Internet assembly 2011: achievements and technological promises*. (2011 ed.). Berlin: Springer.
- Eisenmann, T. R., & Parker, G., & Van Alstyne, M. 2008. Opening platforms: How, when and why? *Harvard Business School*.
- Fisher, C. 2007. *Researching and writing a dissertation: A guidebook for business students*. Upper Saddle River, NJ: Prentice Hall
- Greenwald, G. & MacAskill, E. 2013. NSA Prism program taps in to user data of Apple, Google, and others. *Guardian*.
- Haass, R. C., & Abelson, D. E., & McGann, J. G., & Talbott, S., & Rich, M. D., & Solomon, R. H., & Amus, R. D., & Spring, B., & Betacounrt, A. C. 2002. The role of think tanks in U.S. foreign policy. *Electronic journal of the U.S. department of state*, 7(3): 1-46.
- Hagiu, A. 2006. Pricing and commitment by two-sided platforms. *The Rand Journal of Economics*. 37. 720-737.
- Handley, M. 2006. Why the internet only just works. *BT Technology journal*, 24.
- Huang, Y. & Li, Guanyu. 2010. Descriptive models for internet of things. *IEEE communications magazine*. 13-15.
- Hubbard, K. & Kusters, M. & Conrad, D. & Karrenberg, D. & Postel, J. 1996. *Internet registry IP allocation guidelines*. RFC.
- Isaacson, W. 2014. *The innovators: how a group of hackers, geniuses, and geeks created the digital revolution*. New York: Simon and Shuster.

Jonathan Masters. What is Internet Governance?.

<https://www.cfr.org/background/what-internet-governance>. April 23, 2014.

Kaskinen, T., & Koponen, J., & Lahtinen, V., & Leppänen, J., & Mikkonen, J., & Mokka, R., & Neuvonen, A., & Anttila, J., & Herlin, I., & Kuittinen, O., & Lagus, I., & Noponen, E., & Saarikoski, E., & Vargas, M., & Välimäki, H. ***The future as told through the garden and the streets***. Helsinki: Demos Helsinki.

Komaitis, K. 2008. Aristotle, Europe and Internet governance. ***Global business & development law journal***, 21: 57-77.

Leeson, P. T. & Ryan, M. T. & Williamson, C. R. 2011. Think tanks. ***Journal of comparative economics***, 40: 62-77.

Longhini, A. 2013. ***The role and the influence of think tanks on the policy-making process in Europe. France and Italy's case studies in comparison with the US***. LSE – Paper. The European graduate network conference.

Lyon, D. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. ***Big Data & Society***. 1-13.

Mähönen, P. & Trossen, D. & Papadimitriou, D. & Polyzos, G. & Kennedy, D. 2006. ***The future networked society***.

Mansell, C. 2012. ***Imagining the internet: communication, innovation and governance***. Oxford: Oxford University Press.

Mansell, R., & Steinmueller, W. E. 2000. ***Mobilizing the information society: Strategies for growth and opportunity***. Oxford: Oxford University Press.

Martin, B. R. 2016. Twenty challenges for innovation studies. ***Science and public policy***, 43: 432-450.

McGann, J. G. 2017. 2016 Global go to think tank index report. ***TTCPS global go to think tank index report***, 20: 1-171.

McNutt, K. & Marchildon, G. 2009. Think tank and the web: measuring visibility and influence. ***Canadian public policy***, 35(2):219.

Mendonça, S., & Crespo, N., & Simões N. 2015. Inequality in the network society: An integrated approach to ICT access, basic skills, and complex capabilities. ***Telecommunications Policy***, 39: 192-207.

Missiroli, A., & Ioannides, I. 2012. European think tanks and the EU. ***Bureau of European policy advisers***, 2: 1-51.

- Morelli, B. 2013. *Internet connected devices: Evolving from the internet of things to the internet of everything*. IHS
- Nilsson, N. J. 2010. *The quest for artificial intelligence*. Cambridge University Press.
- Postel, J. 1981. Internet protocol. *International journal of communications, network and system science*, 5.
- Rekhter, Y. & Li, T. 1964. *An architecture for IP address allocation with CIDR*. RFC.
- Rich, A. 2004. *Think tanks, public policy and the politics of expertise*. Cambridge: Cambridge University Press.
- Roberts, L. G. 1967. *Multiple computer networks and intercomputer communications*.
- Selee, A. 2013. *What should think tank do?* Stanford: Stanford University Press.
- Shahin, J. 1999. The internet: a case study for global governance. *Swiss political science review*, 5:120-7.
- Sherrington, P. 2010. Shaping the policy agenda: think tank activity in the European union. *Global Society*, vol. 14:2 173-189. Oxford: Taylor, R. & Francis, W.
- Slevin, J. 2000. *The internet and society*. London: John Wiley and Sons.
- Stone, D. 2000. Non-governmental policy transfer: the strategies of independent policy institutes. *International journal of policy, administration, and institutions*.
- Von Hippel, E. 1988. *The source of innovation*. New York: Oxford University Press.
- Vromen, A. 2010. *Theory and methods in political science*. Basingstoke: Palgrave.
- Weiss, J. A., 1982. Coping with complexity: An experimental study of public policy decision-making. *Journal of policy analysis and management*. 66-87
- Yin, R. K. 1984. *Case study research: Design and methods*. Newbury Park, CA: Sage.
- Zhang, D. & Wang, Z. & Yu, Z. & Zhou, X. & Guo, B. 2013. Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. *Journal of network and computer applications*. 36:1531-1539.
- Zheng, J. & Simplo-Ryl, D. & Bisdikian, C. & Mouftah, H. 2011. The internet of things. *IEEE communications magazine*, 49:30-31.
- Global Commission on Internet Governance. 2016. *One Internet*. Centre of International Governance Innovation and Chatham House.

World Economic Forum. 2016. ***Digital media and society. Implications in a hyperconnected era.***