The Dark Side of the Internet:
A Study about Representations of the Deep Web and the Tor Network in the British Press

by

Thais Sardá

A Doctoral Thesis

submitted in partial fulfilment of the requirements

for the award of Doctor of Philosophy

of Loughborough University

January 2020

Aos meus amados pais,
obrigada por todo o amor e por me ensinarem a sempre
questionar em vez de aceitar as coisas como elas são.
Saudade eterna.

Acknowledgments

During my time as a doctoral student at Loughborough University, I was lucky enough to have the most wonderful people guiding me through the process of becoming a researcher. I am so deeply thankful to my amazing supervisory team, Dr Simone Natale and Professor John Downey, who helped me from the very first email with my research proposal until the very end, reading my work exhaustively and being there for me with professional advice, necessary criticism and words of encouragement. I am thankful also to Dr Richard Bramwell for joining this amazing team and making what was great even better, helping me to deliver the best thesis I could manage to produce. Thank you all ever so much for understanding my pace and believing in me. Thank you also to Professor Sabina Mihelj and Dr Vaclav Stetka for their relevant contribution to this work in their annual reviews. Thank you to Professor Emily Keightley and Professor Tim Jordan for their meticulous review and insightful contributions to my Viva.

I am so proud of my Brazilian background – educação pública, gratuita e de qualidade – as it helps me understand the privilege of studying at a British institution. The School of Social Sciences and Humanities at Loughborough University made this thesis possible through a sponsorship and by providing a network of support that allowed me to present my work around the country and abroad, contributing to my growth as a young academic. My special thanks to the behind-the-scenes women who make this school so efficient go to Elaine Beaken, Ellie Yates, Marie Joyce, Deirdre Lombard, Denise Wade, Louise Lee and Sue Clarke. I am also thankful to the Doctoral College for providing relevant training and giving me with a Santander Mobility Award, and to the Institute of Advanced Studies, especially Professor Marsha Meskimmon and Dr Helen Tighe, for the chance to become a Doctoral Leader.

Thank you to all my undergrad students on the *Sociology* and *Introduction to Research Methods* modules, who taught me how to teach in a new environment and which led to my Associate Fellowship to the Higher Education Academy, and for always providing such kind and generous feedback. I can barely believe that I was so afraid of how people would react to my accent when I arrived in the UK, and now I feel confident enough in my lectures and seminars as

well as have the strong conviction that being a lecturer is one of the most rewarding jobs I could ever wish to have.

On a personal level, moving to the UK changed my life and me. My role as a sub-warden at Elvyn Richards Hall was a big part of this transition, so thank you to the warden Dr Hilary McDermott for taking me in. The best part of this role, in fact, was giving me friends I will treasure for the rest of my life. All my love goes out to my Village Park family, who filled my days and nights with friendship and laughter, especially Fabio, Steph, Leyla, George, Jake, James, Tom and Daniel. As an international student, I looked for comfort and understanding in the Brazilian community in Loughborough, and I found true kindness; therefore, a huge special thanks is extended to Fernanda, Marta and Nadyne for their cherished friendship. An extra thanks goes to my informal PhD support network for uncountable cups of coffee and long talks every Friday at my second home in Loughborough, Bom Bom Patisserie.

This thesis was only possible because I have the best family and friends to ask for advice and to feel close, even when we don't share the same territory. Thank you to my family, who understood and supported my decision to move abroad and constantly encouraged me to be the best version of myself. Eu amo vocês, Mi, Maurício, Cine, Leandro e meus incríveis sobrinhos, Cecília, Otávio e Enrico. Thank you to my friends who are always available on WhatsApp groups and without whom I could not survive, from school to college, from my first workplace to the last. I love you because you are there for me on either the best or the worse days.

Thank you to my wonderful fiancée Headley for everything you have done since our first date, for taking care of me so well every single day, from the small to the big things, and giving so many reasons to finish this PhD. I am looking forward to everything that is ahead of us, and I am so excited to spend the rest of my life with you. I love you so much. Thank you for always being there with a cuppa and for giving me the best British family I could dream of.

Finally, being a Latin-American woman finding her way into European higher education is not an easy task, so thank you to everyone who made this a bit less challenging and helped me overcome my personal struggles. Special kindness goes out to every woman, every Latin-American and every academic going through mental health issues out there. You are not alone.

#resist

Abstract

The imaginary of the Deep Web is commonly associated with crime, crypto markets and immoral content. However, the best-known Deep Web system, the Tor Network, is a technology developed to protect people's privacy through online anonymity, in the context of the contemporary culture of surveillance, thus enabling civil liberties. To understand this contradiction, this thesis looks at the British press representation of the Deep Web and the Tor Network. An extensive empirical research study unveils how newspapers portray these technologies, by looking at meanings, uses and users. In order to meet this goal, this research conducts a content analysis of 833 articles about Deep Web technologies published between 2001 and 2017 by six British newspapers – tabloids *Daily Mail*, *Daily Mirror* and *The Sun*, and quality newspapers *Daily Telegraph*, *The Guardian* and *The Times* – and a critical discourse analysis of 58 reports mentioning the Tor Network, issued by the same newspapers, between 2008 and 2017. The findings demonstrate that the British press represents the Deep Web in a sharply negative way, through negative concepts, definitions and associations. This portrayal attributes opacity to the Deep Web, engendering distrust of its uses and propagating user stereotypes that reflect an overall criminalisation of privacy. Also, the press presents a hyper-panic approach by consistently connecting this new medium to well-known social anxieties and portraying these technologies as undesirable, immoral and illegal. Hyper-panic is the theoretical contribution of this thesis and can be explained as the way in which media panic (the Deep Web, in this case) multiplies moral panic (for instance, terrorism, paedophilia and drug consumption). Specifically about Tor, this work concludes that the media present multiple aspects of this system, from discussing the ways in which one can enable civil liberties, to condemning criminals hiding behind technology, addressing the inherent ambivalence connected to the uses of online anonymity, i.e. it is neither completely bad nor completely good. The general synopsis about Tor, however, is still negative. Finally, the consistent association by the British press between the Deep Web and criminal and antisocial behaviours promotes a dissociation between the Deep Web and the Web itself, in that cyberspace is separated between negative uses (the Deep Web) and positive uses (the Web), instead of being understood as a nuanced whole.

Table of Contents

List of Figures

List of Graphs

List of Tables

Introduction

Conceptualised as the portion of the Internet that is not crawled or indexed by regular search engines (Bergman, 2001; Sui, Caverlle & Rudesill, 2015), the Deep Web is a complex and multifaceted environment that requires multiple perspectives and considerations. From a technical angle, for instance, its study provides a better understanding of how the black box of the Internet works. From a social perspective, the Deep Web is connected to important ongoing discussions about positive and negative uses of encryption and algorithms and how online anonymity can be integrated within everyday life. From a cultural point of view, it promotes the development of new communities and practices in cyberspace, whereas it also helps to unveil the extent of the digital impact on contemporary Western societies. From the economic side, crypto markets and crypto currencies utilise Deep Web systems and environments to propose a new trade logic. From a political dimension, these technologies enable citizens, not only of authoritarian regimes but globally, to exercise civil liberties and access free information. Moreover, the Deep Web is related to rethinking the structure of the Web, challenging the algorithmic norms of the Internet and offering an option to people who are just not interested in the usual services provided by Google, Facebook, Amazon and others. However, if the Deep Web entails such different meanings and implications, why is this technology predominantly represented in univocal ways, stressing its negative uses and criminal associations? Why is the Deep Web defused into the so-called “Dark Web,” a term that invites fear and suspicion, as the next cartoon, drawn by Cathy Wilcox, insightfully demonstrates?

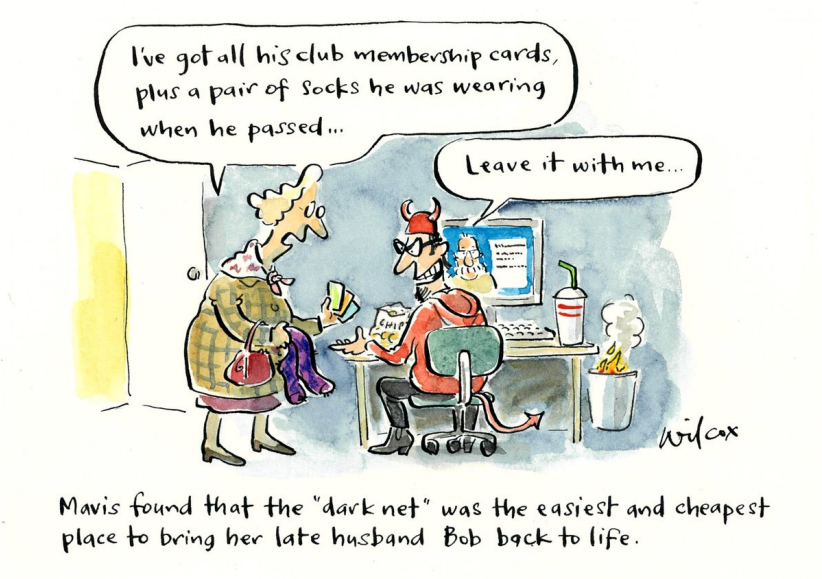


Figure 1: Cartoon by Cathy Wilcox
Source: https://www.cathywilcox.com.au/
Retrieved by the author in December 2019

Let us take a moment to appreciate three core points in this cartoon. Mavis is represented as an elderly woman who is lured by a clearly false promise and, naively or due to a lack of technical knowledge, believes so much in what is offered to her that she is willing to provide any personal information in exchange. Mavis is a representation of the regular Internet user with no particular technical skills and who is fascinated by the Web's potential. The devil is a male hacker, as the glasses stereotypically imply, a person with the technical knowledge but who uses it in order to lure people to give access to personal information, presumably for evil purposes. Finally, the Dark Net is the reason why Marvis and the hacker are connected and an environment where crimes can happen – in this case, the cartoon infers that the identity of the deceased Bob is about to be stolen. Certainly, regular users, hackers and scams are also part of the Surface Web, but this cartoon provides an additional dimension to the humour by mentioning the Dark Net: ultimately, who would believe in anything that is offered on this very nebulous part of the Internet? In fact, these technologies are commonly seen through a combination of excitement and reservations. The same can be said about the Tor Network, a Deep Web technology that was developed to protect users' privacy by providing online anonymity. Tor is considered a threat for those who

follow the maxim “nothing to hide, nothing to fear,” although this rhetoric is associated with authoritarian regimes (Haines & Wells, 2011) and even the Nazi propaganda.

This cartoon is just an example of how the Deep Web is represented and imagined in popular culture, and it shows an evil connotation attributed to these technologies. This approach prompts a relevant question: does the same connotation emerge in the way the media portray the Deep Web? Answering this question is the central aim of this research, and it will be achieved through the analysis of the British press representation of the Deep Web and the Tor Network. Moreover, besides improving our understanding of how these platforms are portrayed, this research aims to position the Deep Web in the context of the imaginary of the Web, which raises a number of other enquiries: how do the media construct the concept of the Deep Web? How do conceptualisations of the Deep Web affect the meanings and imaginaries of these technologies? What are the common topics the media associate with the Deep Web? How are these topics addressed, explained and discussed? How does the press present users of the Deep Web? And what is the representation of the Deep Web in relation to the Web? These questions inspire the analysis herein.

This thesis aims to achieve a greater understanding of the Deep Web’s portrayal by looking at how British newspapers represent and discuss these technologies, drawing on extensive empirical research to unveil the terms through which the press presents them and examining meanings, uses and users. This research relies on a content analysis of 833 articles about Deep Web technologies published between 2001 and 2017 by six British high-circulation newspapers – tabloids *Daily Mail*, *Daily Mirror* and *The Sun*, and quality newspapers *Daily Telegraph*, *The Guardian* and *The Times* – and a critical discourse analysis of 58 reports mentioning the Tor Network, issued by the same newspapers, between 2008 and 2017. These newspapers represent the higher daily reader reach titles in the country, considering a diverse range of political views. Related to this period, each time frame seeks to include the totality of articles published about these topics in the newspapers – from the first publication (2001 in the case of the Deep Web, and 2008 in the case of the Tor Network) to the end of data collection (last day of 2017).

On the matter of originality and what this study offers to the Social Sciences community, it provides a number of original contributions that, at the same time, motivate and justify this

research. The most evident impact is filling a gap in the academic literature with empirical research that unveils and analyses in depth the media representation of the Deep Web and the Tor Network. Therefore, it contributes to the overall Deep Web literature, with a focus on media representation. Using the case of British newspapers, this research provides relevant insights into how the media conceptualise and describe these technologies in terms of meanings, uses and users. Moreover, this analysis places the portrayal of the Deep Web as a new medium, and, broadly, examines how this affects the overall imaginary and representation of the Web. Looking not only to the general case of the Deep Web, but also to the particular example of the representation of the Tor Network, this research also contributes to unveiling the discourse used by the British press about this technology.

In addition, this thesis offers an original theoretical approach in the field of media studies with respect to how new technologies are represented, discussed and associated with social fears. As a theoretical innovation, the findings of this research instigate the development of the hyper-panics concept. In summary, this concept combines media panic and moral panic to describe a phenomenon in which a new medium is seen as a threat (in the case of this work, the Deep Web), not only due to its affordances, but also because it magnifies well-known social fears (for instance, anonymity facilitating terrorism, paedophilia and the drugs trade).

In terms of academic audience, this research could be of interest to scholars within multiple fields. For what concerns media studies, it presents an extensive examination of British newspaper content and discourse and provides an overall picture of how the media signify a new medium, the Deep Web. For surveillance studies, the discussion in this thesis reflects the approach of newspapers to the use of technology to assure the right to online privacy and anonymity; it should be noted that surveillance scholars have a blind spot in terms of the media representation of surveillance, to which this thesis adds a relevant contribution. Finally, for digital studies, this work presents an in-depth analysis of the Deep Web and the Tor Network's meanings and uses, arguing also about the overall imaginary of the Web as well as the portrayal of a new technology. Considering that the imaginary of the Web changed over time, this thesis explores a recent shift in which the Deep Web is seen as "the dark side of the Internet."

Regarding this thesis' structure, in order to identify how this topic has been academically examined to date, an overall literature review is spread over two chapters. Chapter 1, entitled *Imaginary and Media Representations of the Web*, focuses on general concepts that help unveil approaches to the imaginary and media representation of the Web, to position and contextualise the general contributions of this work. The aim of the first chapter is to provide broader concepts and understandings that connect the empirical analysis. Entitled *Surface, Deep and Dark: The many Faces of the Web*, Chapter 2 focuses on relevant aspects of the discussion about the Deep Web, including an overview of surveillance and privacy in the digital era, the technical aspects of these technologies and an examination of different social uses. The goal of the chapter is to provide specific knowledge on the topic of this thesis, which contributes to further understanding of the discussions. In addition, these two chapters act as an initial overview of topics related to multiple discussions throughout this thesis, and are thus necessary to gaining a broader understanding of this matter, but each analytical chapter also presents specific concepts that will help the reader comprehend the details within each discussion, such as the concept of the media and moral panic in Chapter 5, and the concept of liberation technology in Chapter 6. This structure provides a clear organisation of relevant readings related to the thesis as well as to specific chapters, thereby allowing comparisons and associations between ideas, as well as a deeper and broader discussion.

Chapter 3 presents this thesis' *Methodological Framework* through a comprehensive explanation about the parameters within which this work is developed, including not only the research methods applied, but also the basis on which it is founded. The chapter presents the research problem, general and specific objectives and research questions that guide the study, as well as the findings discussed in each analytical chapter. The methodological chapter also offers: the criteria that guided sample selection, in this case six British newspapers with distinct political affiliations and natures (tabloid or quality); the challenges of data collection, including the selection of 27 keywords used to refer to the Deep Web and included in this research; considerations about the time frame, which was not actually limited but reflects all the occurrences of these keywords, since the first publication is attributed to *The Guardian* in 2001, and the use of the software Lexis-Nexis as a means of accessing the content, a total of 833

newspaper articles. Specifically about content analysis, this chapter reviews this method and adds to this details involved in constructing a codebook – in this case, composed of 22 variables and attached to this thesis as an Appendix – and underlining the experience of conducting such extensive coding. Regarding the second method used herein, namely critical discourse analysis, the methodological framework establishes the reasons why this is a suitable choice for this research and how the sample was narrowed down to 58 reports including the term "Tor Network" (or synonyms such as "The Onion Router," "Tor Browser," etc.). This chapter also addresses the ethical implications of this research, by considering that the Deep Web is constantly portrayed from a negative perspective connected to antisocial and criminal behaviours.

Concerning the findings of the empirical research, this thesis considers and discusses them across four analytical chapters. Each of these chapters presents a brief introduction to the topic, including additional concepts that are not addressed in the literature review, the results of the empirical research associated with the analysis per se and a final discussion. Furthermore, these analytical chapters follow a logical order, to provide a broader understanding of Deep Web technologies. The first of the four chapters explains the concepts and attributes that construct meanings, and the second addresses topics that the press associate with these technologies. The third highlights the terms in which there are positive approaches to the Tor Network, and finally, the fourth chapter discusses media polarisation and technological ambivalence in terms of the discourse about Tor. Each chapter is briefly explained in the next paragraphs.

Entitled *The Struggle in Defining Meaning and Concept: A Deep or a Dark Web?*, Chapter 4 focuses on how British newspapers use terms, concepts and definitions related to the Deep Web over time, considering those adopted between 2001 and 2017, to reveal how these technologies are defined and represented by the British press. Since these concepts are related to the construction of meaning of these technologies, and in a subsequent stage their own uses and users, Chapter 4 discusses not only print media struggles in explaining the Deep Web to readers, as well as concepts such as the Dark Web, but also the power of language in constructing an idea of something opaque and negative. In addition, this chapter addresses findings from content analysis to discuss the imaginary of the Web and its positive and negative associations, in order

to investigate the construction of the imaginary of the Deep Web, including the preference of the media to utilise specific metaphors and the adoption of terms such as "Dark Web" and "Deep Web" interchangeably.

Chapter 5 is entitled *"This is the Wild West": The Deep Web and Hyper-Panic* and addresses the elements through which British press coverage associates fear with Deep Web uses. This research suggests that the panic rhetoric surrounding the Deep Web not only focuses on the new medium itself, but also multiplies and increases numbers of other well-known social fears. This chapter draws on content analysis findings to discuss these multiple threats associated with Deep Web technologies, with the aim to define what aspects the British press highlight, and to investigate to wat extent social fears appear in their coverage. The findings of this chapter are related to episodic coverage concentrating on negative uses and criminal associations, common activities mentioned in headlines, official sources and their views and rhetoric and terminologies that the media apply to represent users. This chapter presents a new concept named "hyper-panic," meaning that media panic acts to magnify other forms of moral panic: primarily, media panic is related to the technology's affordances per se, and secondarily, moral panic applies to well-known social fears that the new medium can enable or facilitate.

While previous chapters provide evidence that the Deep Web is mostly portrayed in sharply negative ways, Chapter 6 – entitled *The Tor Network and the Dream of Online Freedom* – focuses only on articles published in tabloid and quality newspapers specifically about positive uses of Tor. In fact, this chapter looks at articles in which Tor is described in affirmative tones, to understand the aspects of a positive approach to this technology. As the analysis shows, in a limited amount of cases, newspapers adopt a liberation technology discourse in their coverage, describing Tor as a means to achieve online freedom and a technology developed against state censorship and private corporations' surveillance, in terms of protecting privacy, assuring anonymity and defending civil liberties. This chapter employs critical discourse analysis to examine 17 newspaper articles from a total of 58 mentioning Tor, and which discuss Tor only in a positive way. This close examination of a relatively small number of articles in the corpus helps understand the nuances of the British press discourse about this technology.

Finally, the last analytical part of this thesis is Chapter 7, entitled *The Tor Network, Technological Ambivalence and Polarisation*. In this chapter, critical discourse analysis shows how the British press deal with multiple perspectives of Tor, in terms of positive and negative uses. In fact, it argues that due to its technological ambivalence, Tor is a complex topic that should be addressed through the usual polarisation that guides the British press. Considering 58 articles about Tor published by six newspapers between 2008 and 2017, according to a preliminary analysis, 15 articles refer to both positive and negative uses, and 12 articles allude to only negative uses. Chapter 7 focuses on these 27 publications. This analysis is relevant to understanding not only how the ambivalence of Tor is addressed, but also how this is used to suggest polarisation. Therefore, the chapter proposes a discussion of the concept of technological ambivalence in the context of the Web, suggesting that acknowledging multiple uses of Tor does not mean unbiased coverage, since polarisation is perceived within the tone of the articles and any associations that are made therein. Finally, considering articles that explore only negative uses of Tor, this thesis investigates to what extent its representation reproduces the overall representation of the Deep Web.

Each analytical chapter proposes particular discussions, and the final *Conclusion* provides an overview of this thesis' achievements in relation to the proposed research questions. In summary, the Deep Web has a negative representation in the British press, which gives a dimension of darkness and criminality to these technologies while portraying them as harmful, inexplicable and opaque. In fact, the British press consistently connect the Deep Web to social anxieties, representing these platforms as undesirable, immoral and illegal, through episodic coverage that reinforces negative uses. This consistent association between the Deep Web and criminal and antisocial behaviours promotes a dissociation between the Deep Web and the Web itself: as the imaginary promoted by the British press, the Deep Web is a place for evil activities, and the Web is a legitimate and positive space of interaction. Specifically about Tor, the media present multiple aspects of this system, from discussing the ways in which it can enable civil liberties, to condemning criminals hiding behind technology, which shows that there is an inherent ambivalence connected to the uses of online anonymity, i.e. it is neither completely bad nor completely good.

Ultimately, this thesis proposes an analysis of the Deep Web and the Tor Network's representation by the British press as a way of discussing and, optimistically, demystifying these technologies. Considering the level of surveillance to which contemporary societies are imposed nowadays, and the assumption that this will grow exponentially, privacy-enhancing technologies have a relevant role in offering alternatives to people to escape this ubiquitous surveillance and instead enjoy civil liberties such as privacy, free information and anonymity. Therefore, the social significance of this thesis also relies on unveiling the portrayal of these technologies, in order to contribute to the normalisation of their uses in everyday life. However, the media's approach to Deep Web technologies not only creates fear of the potential uses but also questions users that attempt to avoid surveillance, in a phenomenon that can be seen as a criminalisation of privacy. If the media produce a specific imaginary of these technologies based on negative associations and stereotypes – with which potential new users cannot identify, or even fear –, it is relevant that academic research opens up the debate to show that there are positive and negative uses of online anonymity. Moreover, there are more perspectives and nuances on this topic than the British press are willing to address.

1 Imaginary and Media Representations of the Web

This thesis aims to understand the British press representation of the Deep Web, by drawing on technical, sociological and cultural perspectives. This entails unveiling how the imaginary of these technologies is constructed through the newspapers' coverage, how different meanings of Deep Web-related technologies are introduced, which uses and appropriations are discussed and how Deep Web users are described and represented. The examination of the print media approach to the Deep Web aims not only to illuminate the Deep Web's framing, but also to contribute to the broader discussion regarding the role of discourse and representations of new media technologies – and in particular of the Web. Thus, this chapter presents approaches to the imaginary and media representation of the Web, to position and contextualise the general contributions of this work. Considering the role of the imaginary in social action (Taylor, 2004), the next sections present relevant literature on how technologies, new media and the Web are envisioned. Moreover, the chapter also discusses key concepts related to the media representation of the Web and delves into approaches unveiling how concepts create meaning.

1.1 Imaginary of Technology

From a political perspective, Carpentier (2011, p. 142) defines social imaginary as 'fantasies that enable an overcoming of the lack generated by the contingency of the social and the structural impossibility of attaining reality.' These fantasies are not "mere" representations but have a role in the reality: '[I]n order to make the reality (imaginary) consistent, social imaginaries are produced, accepted and then taken for granted.' Although there is no general imaginary but instead multiple imaginaries, Carpentier (2011, p. 163) argues that there is a dominant imaginary and power can enable a strategy of hegemonising it, thus creating a consensus, a false harmony, which is seen as a post-political approach: "[A] political project that negates what structurally defines the political (namely the existence of antagonism, difference and dissensus), and that posits a particular perspective on social reality as a universal and non-negotiable truth.' Also providing a concept of social imaginary, Taylor (2004, p. 23) reinforces that it is related to the construction of meaning and 'the ways people imagine their social existence, how they fit

together with others, how things go on between them and their fellows, the expectations that are normally met, and the deeper normative notions and images that underlie these expectations.' As also noted by Taylor (2004), the complexity of the social imaginary is related to how people imagine things around them, without restricting it to a personal level; in fact, the social imaginary is constructed, shared and legitimated in the context of the group, and then becoming common practices in a society.

On the concept of imaginary, Malbreil (2007) argues that it is not the reality in itself but a social construct that exists beside, or previous to, reality in the process of comprehending the world. The author characterises it as an idealisation of reality from a specific perspective, although there is a potential to turn this imaginary into reality and integrate the collective memory, which varies from case to case. In this practice of signifying reality, the imaginary affects the way in which, for instance, technology is perceived, influencing the reformulation of this technology's own existence. For Mansell (2012), the imaginary of technology is fluid instead of fixed or general, which means that multiple imaginaries contribute to the development of technologies guiding changes in communication systems, for instance, and not universally. In this sense, the multiplicity of approaches employed to create a sense of technology makes this a dynamic process in which 'the social imaginary is not coterminous with a "vision" or an "ideology" and it does not imply – in the abstract – a particular understanding of power' (Mansell, 2012, p. 34). Although there is a persistent idea of technological messianism, an imaginary connected to 'an immovable faith in the saving capacity of technology' (Malbreil, 2007, p. 28) reinforces the notion that the recent motivations for developing new technologies, as the example of companies such as Google illustrates, are more related to profit than to the ideal of constructing a better world. Mansell (2012, p. 29) affirms that optimistic views of technological development can be dangerous, since 'the prevailing vision of the information society encourages technological innovation with the promise of benefits for all while, simultaneously, it is facilitating persistence of a social order that is complicit in perpetuating social and economic inequality.'

Discussing the connection between technology and society, Stiegler (1998, p. 90) uses the term 'technoscientific imagination' to claim that modern cultures consistently believe in the

power of technology – through the general development of science and new techniques – to solve problems that are imposed on them, and this in turn creates overconfidence, as if everything can be fixed and humanity can overcome anything. More than an external element, however, Stiegler (1998, p. 90) explains that this belief is not related to the technology per se but in fact reflects trust in the power of humanity developing these technologies and creating a 'human technical intervention' to alter the course of nature. In the same direction, Bishop (2019, p. 28) argues that there is an imaginary as well as a myth that technology is going through perpetual innovation, i.e. 'the idea that there will be permanent innovation in all sectors of life,' in which case humanity can achieve anything – it is just a matter of time, research and investment. Discussing these ideas in the context of life and death, Bishop (2019, p. 20) suggests that there is a co-evolution of technology and society, and in this sense 'technological innovation that shapes human perception of time, life, death and meaning.' Furthermore, Mansell (2012, p. 30) claims that the imaginary of innovation in information and communication technologies (ICT) is connected to revolutionary ideas and attitudes, because they potentially reduce costs, transform the logic of information and encourage social changes.

Considering these multiple contributions to the concept of social and technological imaginary, the next two sections address the ways in which this imaginary is constructed in the specific cases of new media and the Web.

1.2 Imaginary of New Media

In June 1992, the North-American novelist Robert Coover published an article entitled "The End of Books"[1] in *The New York Times*, a text in which he explained how the print media were wrongly portrayed as outdated in a 'world of video transmissions, cellular phones, fax machines, computer networks, and in particular out in the humming digitalized precincts of avant-garde computer hackers, cyberpunks and hyperspace freaks.' Considering how fresh the Web was at that point, Coover imagined potential uses and implications of what was a brand new medium and exposed strong concerns, even using a catastrophic narrative and alienating himself from its

[1] Available on https://archive.nytimes.com/www.nytimes.com/books/98/09/27/specials/coover-end.html Access: November 2019.

use: '[A]s I am entering my seventh decade and thus rather committed, for better or for worse, to the obsolescent print technology.' Although this sounds rather dramatic nowadays, Coover's publication exemplifies how the imaginary of new media is constructed in society, and so the way in which an initial perspective of new media is established, which is the focus of this section.

Initially, it is worth mentioning that Scolari (2009, p. 944) defines contemporary new media as a 'new generation of digital media that is no longer based on the broadcasting logic' and that it 'is challenging the knowledge about traditional mass communication,' although it is important to establish that old media such as television or radio were also new media at some point in history. Others (e.g. Manovich, 2002) have also equated "new media" to digital media, although this approach has been criticised due to the fact that definitions of oldness and newness in regard to media are never absolute and always change throughout time and according to different media configurations (Natale, 2016). As noted by Gitelman & Pingree (2003, xii), when a new medium first emerges, it often passes through a phase of 'identity crisis,' which is usually overcome by adapting the medium and its uses to specific categories of public understanding. Simonson (2014, p. 312) uses the term 'rhetorical invention' to refer to a sociocultural process in which concepts help reduce contemporary prejudice against novelty: '[R]eturning to the etymological roots allows us to move invention more solidly into the realm of cultural, ideological discursive reproduction – the dominant, baseline state of rhetorical invention as an everyday practice across cultures.'

Natale & Balbi (2014) argue that the imaginary is embedded in media change, encouraging modifications and evolution, and adding social and cultural dimensions. Therefore, the distinct interpretation of a given technology across time reflects social and cultural constructions; in fact, these dimensions are part of a chain that starts in the imaginary of the technology, goes through different interpretations and uses that can be made of it and results in the technology's social and cultural constructions. More than prophecies about ideas becoming real technological products, Natale & Balbi (2014, p. 205) argue that 'predictions and speculations about future technologies seem to have actually played a role in the research leading to the innovation'; photography and artificial intelligence, for instance, were discussed and envisioned at a conceptual level before the emergence of these technologies. On the role of imaginary in how

new media are actually comprehended, Natale & Balbi (2014) suggest that the release of a new product instigates social imagination, so both adoption and meaning are affected by groups that apply it in different ways, by considering the existence of a variety of possible uses whose openness shapes the interpretative flexibility (Bijker, 1995) of new technologies.

Addressing the relativity of old and new media, the boundaries of which are constructed through users' attitudes and beliefs, and also how new media are inserted into a social group, Menke & Schwarzenegger (2019, p. 665) state that 'there is an appreciation for the benefits of new media once a perspective of situational use and daily practices replaces the often dystopian imaginaries of the negative impact on the abstract level of society.' Still, for Menke & Schwarzenegger (2019, p. 669), although the imaginary of new media is connected in order to facilitate access to information and communications, 'new media are often conceptualized as threats to social norms and inferior to the normative supremacy of old media. This traces back to a romanticizing of old media or old media environments that are then regarded superior in contrast to the cultural imaginary of the dangerous, inauthentic and unnatural new media.' The next section therefore focuses on the imaginary of a specific new medium: the Web.

1.3 Imaginary of the Web

As noted by Mosco (2004), technologies such as computers and the Web are responsible for important myths, visions and metaphors about our time, and the imaginary influences technology's social impact. On the concept of myth, Mosco & Foster (2001, p. 219) claim that they 'are more than fabrications of the truth […] They are a response to the inevitable failure of our minds to overcome their own cognitive or categorical limits to understanding the world.' Nonetheless, according to Mosco (2004, p. 23), social and economic changes enabled by a new technology depend on overcoming its demonisation and sublime – this last concept is related to the wonderment 'associated with the humanly constructed world,' an amazement which affects actual uses of technologies (see Marx, 1964). Malbreil (2007, p. 2) also argues that the Web instigates dreams and nightmares, in that as a 'current source of the imaginary, it is itself resulting from an aggregation of scientific and humanistic Utopias, prophecies and daydreams on which

not a few people would have bet. Its darkest face has been imagined, quite before as it has been revealed by the facts.'

Indeed, the general discourse about technology in the press and other media is often shaped through hopes and fears related to societal, economic and political aspects (Sturken, Thomas & Ball-Rokeach, 2004; Natale & Ballatore, 2014). The Web is a clear example in which representations include the hope of positive uses, for instance as a vehicle for democracy, community and peace (Barney et al., 2016), and the fears of negative uses, such as cybercrime (Bartlett, 2015), trolling (Coleman, 2014) and other nefarious activities. In the case of the Web, however, throughout the course of history, this technology has been heralded in predominantly positive tones through a romantic view of the development of the Internet imbued with principles, freedom and society (Streeter, 2011). In this context, cyberspace is seen as a mythical space, due the power of computer communications and the potential impact on humankind (Mosco, 2004), and the Internet has been styled as a '"self-realizing prophecy": by repeatedly convincing ourselves and others that it is going to be the main tool of a new society, we actually make it happen' (Flichy, 2009, p. 2).

Considering the case of the Web, Malbreil (2007) asserts that this technology has changed human relations and the general rules of socialisation, challenging the ideas of space and time, which is why the imagination about the Internet is overly stimulated. Even now, although the Internet can be considered mature in most "developed" countries, it continues to feed people's fantasies, as it deals with dreams and imagination (Malbreil, 2007). Part of this curiosity is attributed to the fact that this technology was predicted and/or anticipated by different authors in distinct ages, for instance the novelist Jules Verne in the 1860s, talking about a network to send documents through signs, the documentalist Paul Otlet at the end of the 19th century, imagining a telepicture book, and the poet Paul Valery in 1928, talking about ubiquity. Besides, Mosco (2004) argues that cyberspace has been consistently described through metaphors connected to the imaginary, such as the "digital library," the "information highway," "electronic commerce," "virtual community," "digital ecology" and the narrative stream.

In fact, the imaginary affects how technology is perceived, conceived and developed, as an example provided by Mager (2017) clearly demonstrates. According to Mager (2017, p. 257), the

general attitude to data protection in Europe, with the imposition of limits and standards on Web developers, can influence people's imaginary related to privacy-friendly technologies, and so 'Europe can be imagined as embracing data protection, and thus providing a niche in which alternative technology can grow. Companies can build privacy-friendly features into technology and host personal data on European soil, to mention two strategies discussed for reaching this goal.' Still, for Mager (2017), this means that this imaginary can lead Europe to be perceived in a different way – for instance, as more considerate in terms of dealing with users' private information – and fill a leading role in the technological industry, changing the whole Silicon Valley logic. Considering that the imaginary can influence the rise of a new technology, there is a clear connection between how technologies are imagined and represented.

Moreover, technological imaginary is also built and appropriated according to the context, even when transferred from one technology to another through narrative, as in the case of the Internet, i.e. 'long-standing ideologies, metaphors, and cultural concepts that the Web's founding fathers borrowed from the imaginary surrounding previous media and communication technologies' (Bory, Benecchi & Balbi, 2016, p. 1068). While there were certainly negative uses of the Web from its very first days – discussions about the rise of spam in the middle 1990s (Brunton, 2013) are at least one example –, only recently have negative and positive uses become more evenly balanced. In fact, contemporary debates about the impact of the Web include emerging issues such as fake news and their agenda in the context of the media landscape (Vargo, Guo & Amazeen, 2018), the negative social and psychological impacts of social media, especially among youths (Van Dijck, 2013), the lack of protection of users' privacy by giant corporations such as Google, Facebook and Amazon (Striphas, 2015), abuses by governments (Greenwald, 2014) and individual, corporate and governmental vulnerability to cyberattacks (Landau, 2017). Finally, considering this overview about how the Web is imagined, the next section focuses on how it is represented by the media.

1.4 Media Representation of the Web

This thesis examines the media representation of Deep Web technologies, in order to contribute to the discussion on how new media, and the Web in particular, are portrayed and

imagined. In this context, it is crucial to place in perspective concepts related to media representation. When reaffirming reasons why one should study the media, Silverstone (1999) sustains that society depends of information, and media represents a form of comprehending experiences in everyday life. Nevertheless, for Silverstone (1999, p. 8), 'the simple recognition that our media are ubiquitous, that they are daily, that they are an essential dimension of contemporary experience. We cannot evade media presence, media representation.' Discussing the role of media and culture in the political economy, Durham & Kellner (2006, p. xii) argues that newspapers as other forms of 'culture industries reproduce the dominant corporate and commercial culture, excluding discourses and images that contest the established social system. Closer reading of media texts can reveal a wealth of meanings, values and messages, often contradictory.'

The concept of the public sphere, according to Habermas (2006, p. 73), is related to 'a realm of our social life in which something approaching public opinion can be formed,' which relies on freedom of speech and the circulation of opinions, and 'this kind of communication requires specific means for transmitting information and influencing those who receive it.' Newspapers, for instance, are part of the media within the public sphere. It is noteworthy, in this context, that public opinion relates to 'tasks of criticism and control which a public body of citizens informally – and, in periodic elections, formally as well – practices vis-à-vis the ruling structure organized in the form of a state' (Habermas, 2006, p. 73). For Habermas (2006, p. 76), the press was once 'an institution of the public itself, effective in the manner of a mediator and intensifier of public discussion, no longer a mere organ for the spreading of news but not yet the medium of a consumer culture,' but the later model of mass media, centred on commercial gain, mainly focuses on and is guided by private interests.

Discussing the concept of representation in terms of cultural studies through a constructivist approach, Hall (2013) argues that representation uses language to make sense of the material world in the form of symbols and meanings. Acknowledging the complexity of this process and its social impact, Hall (2013, p. 216) affirms that 'representation is a complex business and, especially, when dealing with "difference," it engages feelings, attitudes and emotions and it mobilizes fears and anxieties in the viewer, at deeper levels that we can explain in a simple,

common-sense way.' In this sense, practices related to representation – made through the media with specific intentions behind the discourse – can encourage stereotyping, thereby raising matters of power, such as the idea of hegemony, and other effects, such as fantasies (Hall, 2013). Considering that the agenda transforms language in discourse, in the context of the media their representation is related to prioritising ideas and persuasion (Kidd, 2016). In fact, Hall (2006, p. 164) addresses the discursive aspect of media as 'framed throughout by meanings and ideas: knowledge-in-use concerning the routines of production, historically defined technical skills, professional ideologies, institutional knowledge, definitions and assumptions, assumptions about the audience and so on.'

From Hall's perspective of representation, Orgad (2012) argues that in terms of the media it is a product of the process of representation and meaning in the contemporary media, usually exemplified by the content of texts and images. Also discussing media representation, Kidd (2016) affirms that 'the study of representation has historically been deemed important in the study of communications because of the limited range of available resources we have to produce representations of the world, of people, events and places,' the media being one such example. Discussing the contemporary media agenda, Orgad (2012, p. 25) establishes that media representation is related to power, in that 'power relations are encoded in media representations, and media representations in turn produce and reproduce power relations by constructing knowledge, values, concepts and beliefs.' Moreover, media representation can have a powerful impact, because it relies on nurturing people's imagination related to aspects of everyday life, since 'imagination is a process of negotiation and interaction between personal and collective thinking and feeling' (Orgad, 2012, p. 43), bringing together real and fantastical meanings.

It is also worth mentioning studies on the representation of online social networks, such as Facebook, Instagram and Twitter, and their potential uses. de Vries & Schinkel (2019), for instance, discuss the imaginary of surveillance that surrounds social media applying facial recognition technologies, thereby allowing the rise in 'algorithmic anxiety.' Moreover, as McGregor (2019) argues, social media activity is currently co-opted by journalists in their political reporting to reflect and represent public opinion, which attributes to companies such as Twitter

and Facebook a legitimised role in creating a general idea of public opinion. According to Oz, Zheng & Chen (2018), these two platforms are constantly seen as enabling uncivil and impolite behaviours, which happen in diverse ways according to the social media platform and if the interaction includes strangers. Researching female empowerment initiatives developed through social media as a potential positive outcome, Hurley (2019, p. 4) states that these actions cannot be considered universal, as they are 'configured through offline cultural-historical practices shaped by gendered traditions, social inequalities, postcolonial and neoliberal configurations.' Research also discusses the use of social media, such as Twitter, in relation to the distribution of misinformation, commonly labelled "fake news," inserted into political discussions (Brummette et al., 2018).

An additional body of literature that is relevant to this study is research in the field of journalism studies, which offer relevant theories and ideas that are further discussed in the analytical chapters. Examining the power of journalism and the particularities of the journalistic field, Bourdieu (1998, p. 70) argues that "the journalistic field is the site of a specific, and specifically cultural, model that is imposed on journalists through a system of overlapping constraints and the controls that each of these brings to bear on the others." Therefore, according to Bourdieu (1998), journalists are constantly subjected to the market logic, competition reasoning and pressure for increasing audience; and journalistic practices are related to legitimacy and power in the diffusion of information. Such a particular activity raises a number of questions, reason why the scope and the transformations of the field of journalism studies has been consistently reviewed for decades. As noted by Hartley (2000, p. 39), who focuses on the activity of journalist per se, "journalism studies should take note of what journalists think and do". Hanitzsch et al. (2005, p. 110) affirms that "journalism studies is, by nature, an interdisciplinary field", which incorporates fields such as communication technology, mass communication, political communication, cultural studies, gender studies, among others. In an addition, Cottle (2009, p. 311) reasons that journalism studies must contemplate how issues and crises "become constituted and conducted within media formations and communication flows around the world". Considering the relevance of these and other viewpoints, this research includes punctual discussions related to journalism studies mixed to the empirical analysis that

follows. This thesis addresses newspapers contribution to the moral panics logic (McRobbie & Thornton, 1995); daily production of episodic coverages on the news (Iyengar, 1990; Vasterman, 2005); purpose and relevance of headlines in the journalistic practice (Bignell, 2002; Reah, 2002); use and absence of sources (Kidd, 2016; Welch et al., 1997); construction of bias (Merkley, 2008; Soroka et al., 2018); and others.

Lastly, media outlets play a relevant role in technological imaginary, by introducing novelty to the public through a process of representation that provides culture, meaning and knowledge about the new technology. According to Fürsich (2010, p. 115), 'beyond just mirroring reality, representations in the media such as in film, television, photography and print journalism create reality and normalise specific world-views or ideologies,' but more so, 'since representations can produce shared cultural meaning, problematic (that is, limited) representations can have negative consequences for political and social decision-making and can be implicated in sustaining social and political inequalities.' It follows that researching how the media represent the Deep Web provides relevant insights into the ways these technologies are socially imagined. In order to achieve this aim, however, it is also crucial to explore how concepts are constructed and used to produce meaning, which is the topic of the next section.

1.5 Conceptual History

Part of the analysis presented in this thesis deals with the concept of the Deep Web, the Dark Net and other phrases used to define these technologies. Therefore, it is important to understand the role of concepts in explaining things such as a new medium. According to Loocke (1999, p. 1), a concept can be described as a mechanism in which 'every living system must categorize "things" or "events" into classes that provoke similar reactions,' by considering distinct elements such as abstract, mathematical, linguistic, scientific, etc. In essence, a concept is a label for something that needs to be named. But why do concepts exist? A condition for a system to have concepts is its coherence with the external world, and therefore only things that need to be explained or codified to make sense in the world are conceptualised (Loocke, 1999). In this sense, concepts both organise knowledge about how the world works and give importance to things, because only things that matter and affect society are named.

Adding to how a concept is formed, Bolton (1997, p. 5) explains that it happens 'through the reciprocal interaction of cognitive structures and environmental events,' and so concepts represent the general knowledge about experiences in the world and are constructed through questioning reality. Analysing a concept also requires identifying the purpose of sociolinguistics, which connects the study of language to a better understanding of society. Spolsky (1998) argues that language is intrinsically connected to social structures, because it is a human phenomenon that both provides meaning to social interactions and encourages social relationships: language per se is social information. As Lakoff & Johnson (1980) insightfully show, metaphors are not only a common language resource and part of the conceptual system in which we attribute meaning to things in the world, but they are also pervasive components of everyday realities, because they are related to concepts and terms and, on a different level, to thoughts about a specific concept and actions that are taken in relation to it. Metaphors likewise help to guide the imaginary about a concept, according to Langer (1954, p. 113), for whom 'in a genuine metaphor, an image of the literal meaning is our symbol for the figurative meaning, the thing that has no name of its own.'

Considering a concept trajectory can provide insights into how the object of conceptualisation has changed over time. On this issue, Koselleck (2004, p. 75) argues that semantics has a high impact on social structure, because of 'the autonomous power of words, without whose use human actions and passions could hardly be experienced, and certainly not made intelligible to others.' It explains why concepts can change meaning over time, depending on the social circumstances (Koselleck, 2004, p. 43). Moreover, considering the relevance of concepts in organising knowledge in everyday life, rebuilding the lifetime of a concept with the aim of understanding it better is actually a methodological system that enhances linguistic and semantic analysis in social history, by considering the reception of concepts and social experiences (Koselleck, 2004). In this context, Koselleck (2002) states that both social and conceptual history are intrinsically linked through the discovery of the historical world, made by repetition of facts and stories about events, and cooperate for a broader comprehension of human society. These theories, however, are different in the way they relate to reality: social history is focused on reflecting facts, while conceptual history aims to discuss the linguistic

representation of events, i.e. 'there is always a difference between a history as it takes place and its linguistic facilitation,' claims Koselleck (2002, p. 25).

Although conceptual history was designed between the 1950s and 1960s as a methodological approach, it is still largely applied nowadays to relate language and reality. Müller (2014, p. 76) defines this theory as 'a clarifying function for present-day political theorizing, especially if coupled with a convincing account of present-day understandings of the experience of historical time.' Therefore, it is ideal for grasping lived experiences and theorising about historical changes through reworked concepts. Kelley (1996, p. 39) understands conceptual history as 'a bridge between the old intellectual world of comfortably shared ideas and the new scene, opened by the linguistic turn,' and thus it is a way of cultivating cultural history. In addition, the hermeneutical condition of this method is intrinsically connected with interpretations since the concept's meaning cannot be separate to it interpretation. On the ideological dimension, Melton (1996, p. 23) reminds us that 'the genealogy of an idea or a movement is something distinct from the idea or movement itself,' due to the interpretation of facts. The main reason for this distinction is the way in which the history is told and the past is represented, because it depends of the historian's perspective, beliefs and background and can be distorted accordingly (Melton, 1996). Addressing conceptual history as a methodological approach, Koselleck (2004, p. 79) refers to 'the practice of textual exegesis, specific study of the use of socio-political concepts and the investigation of their meaning thus assumes a sociohistorical status,' because understanding concepts that compose fact is a prior condition to understanding the fact per se. Thus, the analysis focuses on social conditions in which a concept was designed, as well as changes to the concept over time (Koselleck, 2004).

1.6 Conclusion and further Contributions

Through an examination of key strands of the secondary literature, this chapter shows that constructing an imaginary is part of the process through which society comprehends things in the world and attributes meaning to them (Taylor, 2004) in a way that can affect reality, as well as technologies' actual uses and properties (Malbreil, 2007). In the context of technology, this imaginary is fluid and encompasses multiple visions and ideologies (Mansell, 2012), with power

playing a relevant role in finding a meaning (Carpentier, 2011), as well as modern societies' belief that technologies improve reality (Mansell, 2012) through continuous innovation (Bishop, 2019) and the sense that they can solve any problem (Stiegler, 1998). Related to how new media are incorporated into society, the imaginary is confronted with actual uses and understandings (Gitelman & Pingree, 2003) so that the new medium absorbs these ideas to gain social and cultural dimensions (Natale & Balbi, 2014) and overcome fears (Menke and Schwarzenegger, 2019) and sublime (Mosco, 2004). As a technology and a new medium, the Web exemplifies how technologies can stimulate multiple reactions: dreams and nightmares (Malbreil, 2007), hopes and fears (Sturken et al., 2004; Natale & Ballatore, 2014), positive and negative views (Barney et al., 2016; Bartlett, 2015; Coleman, 2014), euphoria to resistance (Paulus et al., 2013). Although affirmative ideas of the Web were prevalent during its initial narrative (Flichy, 2007; Mosco, 2004; Streeter, 2011), recently, negative and positive uses have become more evenly balanced (Brunton, 2013; Greenwald, 2014; Landau, 2017; Striphas, 2015; Van Dijck, 2013; Vargo et al., 2018).

In addition, this chapter also reviews studies about how the media construct representation, by discussing their relevant role in society in providing access to information and discussing others' experiences (Silverstone, 1999). Specifically, newspapers integrate this social system by presenting meanings and values through messages (Durham & Kellner, 2006) as well as being part of the public sphere where public opinion is formed (Habermas, 2006). As the general idea of representation is related to making sense of the material world into symbols and meanings (Hall, 2013), media representation is associated with a hierarchy of ideas and persuasion (Kidd, 2016), and thereby it is connected to power and agendas (Orgad, 2012). In the representation of technology, the media play a significant role by introducing novelty through a process which constructs culture, meaning and knowledge (Fürsich, 2010). Moreover, the process of representation is connected to concepts, which are names for things that need to be explained or codified, to make sense in the world (Loocke, 1999) and signify general knowledge about experiences (Bolton, 1997). Conceptualisation is a process that involves language, which is per se social information (Spolsky, 1998); for instance, metaphors help to guide the imaginary about a concept (Langer, 1954), and the power of words influences the social structure in ways that are

transformed over time (Koselleck, 2004). Conceptual history as a method is related to comprehending lived experiences and theorising about historical change through reworked concepts (Müller, 2014), intrinsically connected to interpretations (Kelley, 1996) that have an ideological dimension (Melton, 1996). In the case of the Deep Web, even the choice of using one or another term in the daily coverage of newspapers, for instance "Hidden Web" or "Dark Web," contributes to a certain imaginary and representation.

Finally, the examination of the secondary literature provided herein helps not only to introduce insightful concepts and theories that guide the empirical research of this thesis, but also to identify gaps that this research fills in the next chapters. In fact, this work contributes a new perspective of media representation and imaginary through the examination of how the Deep Web and the Tor Network are portrayed by the British press over time, providing in-depth data and discussions related to meanings, concepts, uses, users, associations and other aspects. Alongside building new knowledge on the case of Deep Web technologies, however, this thesis also makes relevant contributions to the overall discussion on the general representation of new media – and particularly the discourse about the Web. The emergence of concepts and representations of the Deep Web is in fact an example of how new concepts and notions related to technology are the subject of 'rhetorical inventions' (Simonson, 2014) that contribute to shaping and changing the imaginary related to specific tools and technologies. In the case of the Deep Web, as the empirical chapters will show, the emergence of notions such as the Dark Web and the Dark Net can thus be contextualised in broader changes related to the overall imaginary of the Web, which has recently shifted from an overall positive representation to more balanced representations where negative and "dark" aspects of these systems are increasingly the subject of attention for the media and the public. Considering that this first chapter of the literature review presents concepts related to technological imaginary and media representation, the next chapter presents the research topic in detail, as it provides a thorough background to the technical, cultural and sociological aspects of the Deep Web.

2 Surface, Deep and Dark: The many Faces of the Web

Inserting the query "Deep Web" into Google[2] provides a list of instructions and tutorials: "The ultimate guide to the Deep Web,"[3] "What is the Deep Web and how do you access it?"[4] and "What is Tor? A beginner's guide to the Deep Web,"[5] among many others. Another common occurrence shows a picture of an iceberg with the analogy that, in the Web, what is over the waterline is just a small part of the whole content. Among 14,300,000 results, the most highly ranked ones also include reminders of the risks associated with the Deep Web and tips on "how to search the Deep Web safely."[6] Going through the results, it becomes evident that there is a widespread uncertainty about what the Deep Web really is, hence the need for so many explanations and instructions. The results also suggest that it is an intricate undertaking to access and navigate the Deep Web, and thus it requires a guide; furthermore, content is considered highly mysterious, which is why the user should be cautious and prepared for all sorts of encounters, even undesirable ones. This chapter, in this regard, aims not only to review the literature related to the Deep Web, which serves as a crucial background to this dissertation, but also to clarify some key issues that a reader not familiar with the topic (one that would search "Deep Web" on Google) may need addressing. The chapter therefore presents relevant aspects of the discussion about the Deep Web, including an overview of surveillance and privacy in the digital era, technical aspects of these technologies and an examination of different social uses. The goal here is to provide specific knowledge on the topic of this thesis, which contributes to the further understanding of the empirical analysis.

[2] Available on https://www.google.co.uk/#q=%22deep+web%22 Access: October 2019.
[3] Available on http://www.sickchirpse.com/deep-web-guide/ Access: October 2019.
[4] Available on https://www.quora.com/What-is-the-deep-web-and-how-do-you-access-it Access: October 2019.
[5] Available on http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/ Access: October 2019.
[6] Available on http://fieldguide.gizmodo.com/how-to-search-the-deep-web-safely-1770828854 Access: October 2019.

2.1 The Web, Network Society and Data

To understand the Deep Web, it is necessary to return briefly to the Web's origins. The initial idea of 'a globally interconnected set of computers through which everyone could quickly access data and programs from any site' (Leiner et al., 2003, p. 2) led to the development in the 1960s of the Arpanet, a primary system of networked computers motivated by sharing resources – especially for communication and information – which spawned the Internet as we now know it. From 1989, through work developed at the European Organization for Nuclear Research (CERN), the Internet became more popular, due to the invention of the World Wide Web by the British engineer and computer scientist Tim Berners-Lee. Berners-Lee (2000, p. 4) found a way to link 'all the information stored on computers everywhere' by developing standardised protocols and conventions by which one computer could move data to another one, thus creating a shared network of machines with distinct systems and in locations across the world. As noted by Berners-Lee (2000), the Web's structure is based in three protocols: a uniform resource locator (URL), which provides a unique address for each page of information, Hypertext Transfer Protocol (HTTP), a computational language to create distributed and collaborative information systems, and Hypertext Markup Language (HTML), basically a way for computers with different languages to translate information into a common language and communicate in a network. The combination of these innovations made the Web a space in which information could travel around and exist (Berners-Lee, 2000).

Although the initial idea was to share resources, the Web has changed. At the beginning of the 21st century, it was not only about a channel for networked information, but also an interactive space for communication and data exchange (O'Reilly, 2007). Discussing the role of the Web in global organisation, Barabási (2002) claims that the information explosion entered companies into a new business setting, named the "network economy," in which information is a product, and all industries depend on alliances and adapting to the challenges of the global market. In this sense, the Internet is a human creation as well as a powerful ecosystem, with its own rules affecting social and economic relations (Barabási, 2002). Moreover, Castells (2010) argues for the concept of the network society, related to the new structure of social organisation and practices around digital networking technologies, thus paving the way for a global system

that, on the one hand, cannot the controlled by governments and, on the other hand, excludes people and territories from promoting social, economic and technological inequalities. As noted by Van Dijck (2013), social networking sites have more recently come to populate the Web and today dominate online sociality, defining how and what sort of communication is promulgated. In fact, the culture of connectivity in contemporary societies attributes a valuable meaning to the user's time: the information that users freely give on social media, combined with algorithmic logic, composes a global market controlled by companies such as Google, Amazon and Facebook (Van Dijck, 2013). In general terms, a network society (Castells, 2010) encourages a network economy (Barabási, 2002) supplied by the culture of connectivity (Van Dijck, 2013). These ideas rely on a common point: the value of information.

Data have actually been at the centre of the Web's transformation since the 1990s, with the continuous growth of the number of webpages requiring an organisational system. Google and Bing are examples of a text retrieval web program, in which a keyword provided by the user goes through proprietary algorithms to check their databases for similar content to offer in return (Voorhees, 1999). When someone searches a name on Google, for instance, its algorithms examine its databases and provide results that best match the searched topic, in order of relevance. It is noteworthy that algorithms are encoded procedures based in mathematical calculations able to transform input data into a preferred output (Gillespie, 2012). As noted by Goffey (2008), algorithms combine logic – made by a coded language with a pragmatic dimension – and control – where commanding structures analyse situations and give a response back. A search engine database demands two algorithmic processes (Voorhees, 1999): indexation, which is the selection of terms that best represent content (keywords in an article, for example), and matching, a comparison of text representations (between keywords and related data).

Indexation is a key facet in understanding Deep Web content, as the topics addressed in the following show. In fact, this chapter introduces concepts that are relevant not only to the analysis, but also to the very understanding of these technologies in terms of their purposes and how they work. Before that, however, this literature review focuses on concepts of the culture of surveillance, online privacy and online anonymity to provide a broader understanding of the impact of digital technologies in everyday lives and their social context.

2.2 Culture of Surveillance

Finding an alternative to ensure online privacy and anonymity seems like an impossible job nowadays, considering that surveillance practices promoted by states and corporations are part of everyone's routine when using the Web (Lyon, 2009). The Internet offers clear benefits that facilitate everyday tasks (Van Dijck, 2013). At the same time, these services collect data about the user's behaviour (Lyon, 2009), and these data are at the centre of online surveillance practices encouraged by authorities and private companies (Dinev, Hart & Mullen, 2008), creating a powerful network of information which is the main risk to privacy (Gray, 2003). Lyon (2009, p. 2) reminds us that surveillance 'means "watch over" and as such it is an everyday practice in which human beings engage routinely, often unthinkingly,' which includes a parent looking after a child and a guard monitoring a prisoner in their cell. As these examples imply, surveillance is connected to power, control and fear – and the classic example of the panoptic corroborates this notion. Explaining an idea for an Inspection House building, Bentham (1995, p. 5) described in the 18th century a place 'in which the objects of safe custody, confinement, solitude, forced labour and instruction were all of them to be kept in view' as a way of precautionary contrivance. Based on this principle, the observation per se would assure power and control over the person who is being watched. Foucault (1995) argues that environments with power balances develop surveillance as a means of submission: the panoptic is inherent in the disciplinary power, in which the person watching is invisible and everyone else is under compulsory surveillance. Another idea behind surveillance is described in the book *Nineteen Eighty-Four*, written by George Orwell in 1949, in which the state keeps citizens under control by installing watchful devices in their homes. Lyon (1994, p. 58), however, affirms that Orwell's metaphor focuses on state observation and 'today, surveillance is both a globalizing phenomenon and one that has as much to do with consumers as with citizens.'

In a post-panoptical approach to surveillance, Deleuze (1992) discusses the society of control, a dynamic structure in which public and private institutions cooperate in order to ensure a broader form of surveillance. Nevertheless, for Deleuze (1992), instead of confining a person (as the panoptic approach would argue), the contemporary human being can experience a feeling of freedom while actually being part of a broader mechanism of control in a dispersed and

networked surveillance system that involves every action the person takes through intricate and interwoven cooperation between governments and private companies. As noted by Haggerty & Ericson (2000, p. 619), surveillance combines social practices and technologies, which allows for 'the progressive "disappearance of disappearance" – a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions.' Lianos (2003, p. 418) also points to sociotechnical systems collaborating to create an invisible surveillance network through institutions, thereby producing 'a circularity of reasoning which confirms that the mechanisms of control indeed control effectively, threaten our liberties and lead to totalitarian developments.' Thus, the Internet has changed the way surveillance is undertaken, and using automation engenders a 'growing concern about the degree to which digital media and device networks can be used as tools of social control' (Shorey & Howard, 2016, p. 5032). Macnish (2012) refers to automated surveillance as 'unblinking eyes,' a reference to a clearly non-human quality of observing absolutely everything uninterruptedly.

Moreover, the convergence of technologies is fundamental nowadays to the management and perception of vigilance, by adding power to the surveillance system, which is encouraged by government's monitoring activities and identifying potential threats (Lyon, 2009). In fact, surveillance is largely tolerated in the prevention of crime (Hope, 2009). When a terrorist attack happens, for instance, people increase their tolerance to surveillance, even risking their own civil liberties, which is seen as a side-effect of protecting national security (Lyon, 2009). According to Gray (2003, p. 314), terror acts receive a dramatic narrative in the media, manipulating risk perception, spreading fear and generating a vicious circle, with surveillance 'a reaction to perceptions of insecurity in urban spaces.' Dinev et al. (2008, p. 227) argue that terrorism 'enhances government authority to obtain personal information about consumers from private-sector sources. This evolution in surveillance authority increases the panoptic power of the government.' In intelligence approaches to threats, surveillance can surpass borders and be transnational, in that information flows through systems operating in different geographical locations, and cooperation and data-sharing occur between nations (Wood, 2001).

Private organisations play a role in surveillance by collecting and selling personal data as part of the market logic, as seen in the example of companies such as Google and Facebook (O'Reilly,

2007; Dijck, 2013) that use traffic analysis (Diffie & Landau, 2007). These corporations introduce society into an algorithmic culture 'enfolding of human thought, conduct, organization and expression into the logic of big data and large-scale computation, a move that alters how the category culture has long been practiced, experienced and understood' (Striphas, 2015, p. 396). Considering these interests, Dinev et al. (2008, p. 214) argue that 'both private corporations and government agencies take advantage of the increasing technical capability of information systems to collect and process consumer and citizen data.' Nevertheless, they have different aims: corporations are after 'consumer preferences for commercial purposes,' and the state watches 'citizen behaviours to detect and prevent security breaches, fraud and other crimes, and terrorist activities' (Dinev et al., 2008, p. 214). This combination of agendas is translated into technologies monitoring people constantly, collecting and organising personal data for multiple reasons and making it impossible to escape it in everyday life, leading Lyon (2009) to call it a 'surveillance society.'

In this digital era, a new level of power is attributed to those that hold data, a by-product of surveillance (Gray, 2003). As noted by Gandy (1993), surveillance promotes cultural changes in the treatment of personal information, legitimating consumerism practices and affecting personal privacy. Albrechtslund (2008) defines participatory surveillance as having profiles on social media, using this space to express opinions and interests and to share personal information, interacting with others in public or private spaces. All of this information – which includes images, videos, audio, receipts, tickets and activity records provided to public actors (such as police and border control) or private organisations (such as credit card or social networking companies) – makes each individual identifiable, marked and categorised, thus connecting surveillance strategies to social relations and power (Lyon, 2009). In terms of how surveillance can promote inequalities, this logic discriminates by classifying people with different political, economic and social realities and views in common categories through three processes: identification, classification and assessment (Gandy, 1993). Similarly, Lyon (2009, p. 2) discusses the 'ways in which data are used for "social sorting," discriminating between groups who are classified differently,' and how this hands power to governments and technology companies, and promotes social exclusion.

This background to surveillance studies is relevant to understanding what Lyon (2018, p. 31) calls the 'culture of surveillance': '[T]oday, surveillance is frequently fluid and flexible, in contrast to previous solid and fixed forms, and this resonates with the more liquid modernities of the present. Surveillance works at a distance in both space and time, channelling flows of data and sorting people socially. However, surveillance operates increasingly in consensual ways, dependent on how people perceive and act in relation to surveillance.' In this context, users have a central and active role, in that 'it is mistaken to see surveillance today simply as something that is "done to us"; surveillance is experienced and also initiated by ordinary users. Many people do surveillance themselves, sometimes relying on complex technology to do so' (Lyon, 2018, p. 29). Against this backdrop, pursuing privacy on the Internet is a way of challenging surveillance practices (Dingledine et al., 2004) and compensating for the impact of technology on the right to privacy (Floridi, 2014). It is not a surprise, therefore, that tools utilised to circumvent online surveillance are largely available on the Web (Sui et al., 2015), such as privacy-enhancing systems like the Tor Network (Bartlett, 2015; Jaeger, 2015; Loesing, 2009). Therefore, and considering that Tor's moto is "Browse Privately. Explore Freely,"[7] the next section focuses on online privacy.

2.3 Online Privacy

A broader understanding of privacy-enhancing technologies purposes and uses relies on the construction of the concept of privacy. It is generally defined by Westin (1967) as the personal 'right to control, edit, manage and delete information about them and to decide when, how and to what extent that information is communicated to others.' Altman (1977, p. 67) focuses on relationships to describe 'privacy as the selective control of access to the self' by contemplating three perspectives: a dynamic and dialectic process in which people choose to be accessible to ones and not others; the optimisation of an adequate level of privacy, which varies from crowding to isolation; and multi-mechanism, as multiple behavioural systems help people to achieve social interaction. Reviewing these ideas, Burgoon (1982) explains privacy as existing in four dimensions: physical (presence and location), social (an individual in relation to the group),

[7] Available on https://www.torproject.org/ Access: October 2019.

psychological (affection and cognition) and informational (public knowledge about a person, group or organisation).

In contemporary digital societies, the lack of privacy is a social issue, since 'information technology is considered a major threat to privacy because it enables pervasive surveillance, massive databases, and lightning-speed distribution of information across the globe' (Nissenbaum, 2010, p. 1). For Nissenbaum (2010), however, online privacy is more related to the appropriate use of data than one's own access to data per se. As a result, the problem is not information being gathered but what governments and corporations do with this information (Dinev et al., 2008). This logic considers the current social context in which Internet users actively adopt surveillance practices. Papathanassopoulos (2015, p. 2), for instance, mentions privacy 2.0, a dynamic idea of privacy, by examining changes in the concepts of the public and the private, and also suggesting that 'our personal information has become a commodity that can raise our visibility in the social media driven world.' Chen (2018) also addresses the privacy paradox in social media, i.e. the fact that people can be worried about privacy but still provide personal information, through an extensive empirical research that shows that awareness about privacy risks is generally translated into more cautious behaviours. Discussing how technology promotes the personalisation and customisation of search results, Garcia-Rivadulla (2016, p. 235) states that privacy is 'about transparency in the methods used and the purposes sought. It is about each person's right to decide, free from commercial and governmental pressures and interests.'

In many academic discussions, the threat to privacy is seen as a by-product of a safe country. As Dinev et al. (2008, p. 228) argue, 'a balance between the need for security and the fear about losing privacy exists in society.' According to O'Rourke & Kerr (2017, p. 23), 'the security versus privacy debate is largely state-centric' as a result of the general argument that individual rights cannot prevail against social welfare. In this sense, people should jeopardise their privacy and allow information to be collected, in order to ensure the nation is secure. From a distinct perspective, however, Lippert and Walby (2016, p. 351) 'de-[couple] privacy from individual rights to show that privacy is not necessarily an antidote to surveillance. Rather, when coupled with security and "built in" to technology, privacy can enable surveillance for authoritarian purposes. In some instances, privacy and security become almost indistinguishable.' A counter-

argument is that protecting personal privacy is a way of protecting society in itself, as noted by Nissenbaum (2010, p. 44), who posits that as the space where interactions happen becomes more digital, the way data are shared and analysed on the Web affects socialisation, once 'privacy norms do not merely protect individuals; they play a crucial role in sustaining social institutions.' In fact, Roessler & Mokrosinska (2013, p. 785) discuss a philosophical approach to privacy that goes beyond contrasting individual and social interests whereby privacy has a crucial role in relationships and social interactions, and therefore 'a transparent society, a society without privacy, would be a society deprived of meaningful social relations.' Weinberg (2017, p. 16) affirms that privacy needs to be addressed in the general context of digital economy and not in the individual level, since 'a privacy rights framework risks reducing the totality of the digital economy and its attending conditions of exploitation to a matter of individual rights rather than a social condition.'

A key moment in understanding the current discussions about online privacy is connected to the Edward Snowden revelations in 2013, which helped to clarify and exemplify how governments promote surveillance practices and 'raised important questions about the ability and willingness of states and corporations to protect citizen privacy' (O'Rourke & Kerr, 2017, p. 21). As a whistle-blower, the former agent in the North-American National Security Agency (NSA) confirmed long-term suspicions when he 'brought to public attention the full extent to which data generated by everyday activities on digital platforms can be monitored and used by the state apparatus' (Troullinou, 2017, p. 72). The journalist responsible for the publication of the content in the case, Greenwald (2014, p. 6), admires Snowden for 'daring to expose NSA's astonishing surveillance capabilities and its even more astounding ambitions he has made it clear, with these disclosures, that we stand at a historic crossroad. Will the digital age usher in the individual liberation and political freedoms that the Internet is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control, beyond the dreams of the greatest tyrants of the past?' According to Lyon (2015, p. 94), who refers to Snowden as a 'storm,' these revelations show that surveillance challenges the right to privacy, since 'privacy is also connected with living in a democratic society, where there are statutory limits to what government may do secretly, and where we should be able to disagree with the government without fearing the

consequences.' According to Smith (2018, p. 5), 'in light of Snowden's salient disclosures, it seems surprising that neither widespread boycotts of data sharing technologies and infrastructures have materialised nor more significant uptake of VPNs and the darknet.'

Although vigilance practices have their critics, and there are broad discussions about privacy, a culture of surveillance (Lyon, 2018) has been established and has no anticipated disruptions. O'Rourke & Kerr (2017, p. 34) argue that 'privacy is not being redefined in the context of intercontinental data transfers but rather narrowed to a neoliberal free trade framing of information privacy. State and transnational institutions are exerting influence on the ways in which citizen and consumer data can be used, but they are not radically redefining privacy in a way that challenges existing corporate practices.' This pessimistic approach is supported by Doyle (2018, p. 237), for whom 'it is not that technology is an autonomous, ineluctable force whose ravages to privacy are inevitable. Rather, it is that technology and the information flood that it produces will not in fact be stopped,' because they are supported by economic power. There are, however, some attempts at resistance. The Tor Network, for instance, is motivated by the mission to 'advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding.'[8] Considering this point, the next section focuses on the concept of online anonymity and its distinct meanings over time to become, nowadays, a way of retaking power over personal data and thereby reassuring privacy.

2.4 Understanding Online Anonymity[9]

In 1993, a famous cartoon published in the *New Yorker* proclaimed that 'On the Internet, nobody knows you're a dog.' At the time, the Web was a new technology that seemed destined to open up novel ways to experience identity in interactions with other users. Early adopters were promised the opportunity to employ pseudonyms and anonymity, to play freely with their

[8] Available on https://www.torproject.org/about/history/ Access: October 2019.
[9] An earlier version of this section has been published as Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019). Understanding online anonymity. *Media, Culture & Society*, 41(4), 557-564. https://doi.org/10.1177/0163443719842074

identities (Turkle, 1995). As the Web developed in the ensuing years, new models of interaction and technical solutions appeared, showing the limits of this vision. Since personal identification was becoming a condition for using several services, and the continuities between offline and online identities appeared more contingent, scholars argued for the need to go 'beyond anonymity' (Kennedy, 2006). And yet today, as the Web passes its 30th anniversary, the concept of online anonymity seems again extremely relevant to understanding the social, political, economic and cultural implications of the Internet. The importance of anonymous communications is evident from multiple perspectives. For instance, online anonymity is now regarded as a fundamental factor in the protection of private information and in reducing the dangers of the Web, such as hacking and malware (Hoang & Pishva, 2014), as a facilitator for participation in discussions about sensitive topics – health issues, for instance (McLeod, 2011) – in computer-mediated communication and as an option for citizens to avoid government surveillance in highly repressive as much as highly liberal contexts (Jardine, 2018b).

Since the emergence of the Web, then, much has changed that makes it necessary to revise basic assumptions around anonymity and the Internet. Arguably, the main dynamic igniting such change is the development and the increasing availability of new technical means that enable different degrees of online anonymity. This can be achieved in different ways and through the use of a wide range of tools, including functions on the most widespread Internet browsers – such as the Incognito tab on Google Chrome – proxies, virtual private networks (VPNs) and the Tor Network, a browser employing multiple layers of encryption (Hoang & Pishva, 2014). The emergence of such technical tools forces us to reconceive online spaces as contexts in which different levels of anonymity and pseudonymity are performed through technical means, and to reflect more structurally on how both the technical and the social dimensions inform the constructions of identity and the performance of privacy online.

A lively debate amongst policymakers, security professionals, hacker communities and human rights associations has recently ensued regarding whether online anonymity is acceptable and, if so, in what form. If online anonymity is related to both social and technical issues, how should the role of these two different dimensions be investigated? This question emerges from the tradition of social studies of media and communication that refuse to give primacy to either

technological or social factors but instead insist on the necessity to acknowledge and study how change emerges from the interactions between technology, society and culture (Williams, 1975). It is necessary, in this sense, to avoid a perspective that privileges one or the other dimension, instead developing an approach that looks alternatively at their mutual interrelations.

From a technical perspective, anonymous communications on the Internet can be achieved to different degrees, using technologies such as Internet browsers, proxies, VPNs and Tor (Hoang & Pishva, 2014). For users who place a premium on privacy, one of the most established anonymity-granting technologies is The Onion Router (Tor), a browser that ensures a level of confidentiality by linking a network of computers, thereby providing layers of encryption between the user and the information source and making it very unlikely for someone to trace back both sides (Minárik & Osula, 2016). Although Tor is functionally neutral, since anonymity can be applied in multiple ways and shaped according to distinct purposes, there are two common uses of this technology: first, as a resource to circumvent political repression, especially in highly repressive contexts, in order to exercise freedom of speech, and second, as a new way to engage in illegal activity, taking advantage of online anonymity to escape law when committing crimes (Jardine, 2018b). In fact, Tor is widely known for its illegal uses, and websites on this network are generically referred to as the "Dark Net." Despite the variety of content available through Tor, emphasis is often given only to crypto markets such as Silk Road, the most notorious online drug marketplace, which connected thousands of sellers and buyers using Tor and allowed them to preserve their identities from 2011 to 2013 (Aldridge, 2019). These issues are addressed in this literature review.

One anonymity-granting resource that is commonly available and widely used is VPN services, which can change a user's original IP address for another one in another location, typically offering multiple geographical locations around the world from which to choose. As a result, tracking the user will lead to the IP address but not to their computer, i.e. a server provided by the VPN. Data protection through VPN services has one primary advantage from a privacy point of view, in that all the information shared by the user, regardless of the applications, is immediately encrypted and dispatched through a secure tunnel established by the VPN server. Due to the centralisation of information ensured by VPN companies, however, this service alone

is not considered completely secure. For instance, users' data may be used by this company for marketing purposes, or data about users may be released to authorities upon an official request (Hoang & Pishva, 2014).

Another key tool for privacy is end-to-end encryption, a form of electronic cryptography that works through a secret key shared by the sender and the receiver. This is a 'core technology for data security and data protection and therefore constitutes a central component of the technical infrastructure of information society' (Winkel, 2003, p. 185). The instant messaging and calls service WhatsApp, for instance, employs such technology, meaning calls and messages posted by users are secured with end-to-end encryption. This implies, according to WhatsApp (2018), that all communications via this platform are protected from third parties, so that nobody apart from the sender and the receiver can access the content – not even WhatsApp (or Facebook, which owns this company). The same applies to the content of other messaging and email services, such as Gmail, which also offers a system of protection, including in-transit encryption, to preserve messages from interception.

Online anonymity, however, is defined as much by technical means as by social uses and understandings. If technology provides multiple ways for users to protect, at least in part, their identity online, the ways through which users appropriate these technical tools are manifold, too. Given that privacy is related to control over personal information about oneself, and the right to decide how this information is available to others (Westin, 1967), anonymity is usually employed as a form of privacy enabler in the context of the Internet. In this regard, depriving the Web of one's personal data is a way to counterbalance the impact of online technologies, thereby imposing a limit to the surveillance logic (Floridi, 2014). In terms of social uses, Wu & Atkin (2018, p. 4526) argue that there is a 'positive relationship between online anonymity and the likelihood of opinion expression.' Besides, Sharon & John (2018, p. 4190) note that anonymity enables 'users to disclose more openly than on other social media platforms, to express unconventional opinions, and to experiment with a wider range of aspects of their identity.' More broadly, however, online anonymity can be arguably compared to a weapon: on one hand, it can be used to harm, but on the other hand, it is an instrument for self-defence. In fact, as a double-edged sword, online anonymity may help whistle-blowers remain safe in totalitarian states, but it may

also enable bullies to evade punishment. This has made the discussion about the social applications of anonymity in a context of interconnected surveillance particularly polarised (Jardine, 2018b).

While anonymity plays a relevant role in the development of communication and collaboration tools, privacy-enhancing technologies are also regularly appropriated as a support to criminal activity. Illicit uses of online anonymity challenge the authority of law enforcement agencies s and restructure power relations and legal norms on the Internet, because the ability to hide the identity that protects users from prosecution can be used on multiple levels, such as creating new and more efficient forms of cybercrime (van Hardeveld, Webber & O'Hara, 2017). This in turn allows for the existence of drug crypto markets that capitalise on the anonymity tools (Martin, 2014; Morselli et al., 2017), adding sophistication to the hacking attack technology (Hoang & Pishva, 2014) and facilitating illegal file-sharing, a practice that has been constantly growing on the Web (Larsson, Svensson & Kaminski, 2012).

It is not only users' use of technologies, but also their understanding and knowledge of these systems that informs online anonymity. As noted by Park (2011, p. 232), 'knowledge plays a critical role in privacy behaviour, the levels of understanding of surveillance practices common in websites remain miniscule among the majority of users.' For this reason, promoting digital inclusion and reducing online inequality includes discussing issues such as privacy and surveillance (Gangadharan, 2015). In addition, Jordan (2019) demonstrates that people define anonymity in different ways, and as they navigate the Internet, use social media or download a pirate copy of a film, they might have different degrees of consciousness about the extent to which their identity is exposed – or not. Users, for instance, might have the misguided belief that they are browsing completely anonymously when using the Incognito window on Google Chrome, while not even a sophisticated system such as Tor might seem safe enough to a skilled user seeking to escape surveillance. Not only rational choices, but also emotions and affect play a role in these dynamics (Kennedy, 2006). By the same token, anonymity constantly intertwines with issues of race, gender and class. Even though visual and aural clues that mark people's identities in the offline world may be invisible online, even anonymity and pseudonymity do not allow one to escape completely a 'real world' identity (Kolko, Nakamura & Rodman, 2013).

Finally, the social dimension of online anonymity also concerns representations that are given in the public sphere of issues related to online anonymity. In recent years, online spaces of anonymity have been often described through the Dark Web label, and usually described in negative terms as an obscure part of the Web exploited for illegal activities and endeavours. As this research shows, after the analysis of 833 articles published between 2001 and 2017 in the British newspapers *Daily Mail*, *Daily Mirror*, *Daily Telegraph*, *The Guardian*, *The Sun* and *The Times*, representations of the Dark Web are underpinned by a sharply negative characterisation positing a strict link between online anonymity and criminal or antisocial activities. Counteracting the positive and optimistic representations of the Web as the harbinger of personal freedom, participation and democracy, online anonymity is thus presented as being related to the 'dark side' of the Web (Brunton, 2013; Flichy, 2007). This may ultimately have an impact on uses and understandings of online anonymity, not only because media representations inform people's understandings and behaviour, but also because discourses about the Internet inform public policies and may therefore have practical consequences (Crawford, 2007).

While it is important to highlight different dimensions of online anonymity, the study of this phenomenon cannot be conducted by considering any of these elements alone. Technical issues, uses, understandings, representations and policies are strictly interrelated, and it is within the space of their interrelations that anonymity is experienced and operationalised online. We propose, therefore, that the study of this phenomenon should rely on a deep understanding of the fluid nature of online anonymity. This implies that technical and social aspects are never to be taken as a given, because their meanings and implications only emerge from the mutual interactions between these dimensions.

Debates about online anonymity are often characterised by a high degree of polarisation: on one side, critics call for more restricted regulations of anonymity-enabling tools and send out alarm calls for the questionable uses of online anonymity, such as the lack of accountability on the publication of sensitive information by WikiLeaks (Zajácz, 2013); on the other side, supporters of the right to anonymity emphasise the positive role of anonymity in enabling privacy and political freedom (Jardine, 2018b). A way to resolve whether claims to online anonymity are legitimate is to see this within the context of individual rights. Such rights are, or should be,

absolute; yet, at the same time, they are contextual. As legal theorist Tara Smith (2017) mentions, while examining whether the right to freedom of speech is an absolute, 'rights that allowed a person to infringe on others' rights would kill the protection – the recognition of moral title – that the idea of rights affirms.' Thus, someone's right to freedom of speech is indeed absolute, and yet it does not allow that person to send death threats. In the same way, the right to property does not allow someone to loot their neighbour's garden and then deny entry to the police.

Consequently, one's claim to privacy or anonymity could be seen as a derivative of basic rights, such as the right to property: individuals own their computers, and therefore any data therein should be excluded from the view of other parties (except when the owners have consented to it). Yet, such a right no longer applies when someone infringes someone else's property rights, such as in the cases of downloading copyrighted material. However, the issue becomes more complicated by the fact that there is no consensus on (a) what constitutes one's fundamental rights and (b) what the role of the government should be in a rule of law society. Thus, one can see drug traders in crypto markets claiming they are only engaging in peaceful voluntary interactions which have positive externalities, such as a reduction in street drug-related crime, whereas prosecutors could at the same time claim that the individual right to peaceful trade is inferior to society's claim to maintain some moral codes that exclude the free trade of substances (Sotirakopoulos, 2018).

Overall, while the use of different anonymity-enabling tools will be more and more essential to avoid omnipresent surveillance and to enable political activism on the Internet – as Coleman (2019) convincingly argues – the polarisation between critics and supporters of the right to online anonymity fails to consider that online anonymity is not one thing but many; or, more precisely, that online anonymity is an inherently fluid concept whose meaning can only be established through the examination of specific contexts and situations. In fact, different technical tools are given different meanings and bring forth different results based on the distinctive uses, understandings, skills and knowledge of each user, on the tools employed with the different degrees of anonymity they enable and on the particular situation and context in which these tools are employed. Acknowledging the fluidity of online anonymity means defining it not as an absolute condition but rather as a wide space of movement within which users make different

choices to protect their identity and privacy. Indeed, looking at the social and cultural dimensions of anonymity, scholars such as Turkle (2005) and Papacharissi (2002) attribute to anonymity the online reinvention of the individual, and therefore the combination of user and machine creates a new self that is shaped by sociality as well as by the technical affordances of online spaces.

One of the consequences of this approach is that, contrary to ongoing discussions of online anonymity that characterise this issue as relevant to the actions and motivations of specific groups of users such as hackers, criminals, activists or journalists, one should acknowledge that it characterises to a certain extent any kind of online social interaction. Whenever users connect to the Internet, degrees of anonymity and non-anonymity are established that contribute to shaping their experience, its implications and effects. Understanding the fluid nature and the everyday character of online anonymity, in this sense, provides an antidote to approaches that ascribe rigid values to it, denouncing it as a security threat or heralding it as a panacea against surveillance in the Web.

2.5 The Deep Web

To understand the Deep Web, it is necessary to review ideas and concepts related to technical aspects of the Internet, for instance how search engines work. As noted by Olston & Najork (2010), a web crawler, also known as a "robot" or a "spider," is a programmed system that automatically reviews webpages with the purpose of indexation, web archiving, web data mining, web monitoring services and others; ultimately, web crawlers are algorithms responsible for aggregating content to be used by search engines. However, these algorithms cannot collect absolutely all the information available on the Web. The content that is not indexed, and therefore not found by web crawlers over the Internet, is called the Deep Web (Bergman, 2001). As the iceberg metaphor indicated above (see Figure 2), available information on the Web can be divided into two portions: above the waterline, known as the "Surface Web," consists of all content crawled and indexed by standard crawlers, used by search engines and accessed through web browsers such as Internet Explorer and Google Chrome, while below the waterline is the Deep Web, 'the portion of the Web that has not been crawled and indexed, and thus is beyond the sonar reach of standard search engines' (Sui et al., 2015, p. 6).

Figure 2: Structure of the Web represented by an iceberg
Source: designed by the author

The fact that this content is not found by crawlers, even when they apply advanced and sophisticated technology, depends on the web developer's decision to create a non-crawlable webpage, by limiting access through a password or encrypted gateway software, or by specifying in the code that the page should not be crawled (Sui et al., 2015). A company's intranet accessed only through a staff login and with private content not indexed by search engines is considered the Deep Web, for instance. The same logic applies to sites or digital repositories only accessed by a specific browser or system that the common search engines cannot index. This raises the question as to what is available on the Deep Web. As noted by Bergman (2001), the main categories of content are: topic databases, a subject-specific aggregation of information; internal sites, with searchable databases dynamically created; publications; shopping and auctions; classifieds; portals with more than one of these categories; libraries with searchable internal holdings; yellow and white pages (people and business finders); calculators with an internal data component for computing results, such as translators; jobs; message services or chat and general

searches in relevant databases. This content can be useful for a series of reasons, interests and purposes. According to The Tor Project[10], the most well-known tool for Deep Web users, as explained in the next section, is user feedback,[11] which means that journalists can adopt the Deep Web as a door to free information and multiple perspectives on controversial topics. In fact, institutions such as Reporters Without Borders[12] even advise sources and dissidents to use Tor, in order to avoid surveillance. The same applies to activists and whistle-blowers fighting for freedom of speech, human rights and transparency against states or corporations. The Deep Web also has corporate purposes, allowing repositories of sensitive information to resist cyber-attacks, and military, since field agents can use Tor to disguise communications, thereby protecting themselves, information and operations. It is relevant to mention that Tor can also have opposing uses, one of which is indeed criminality (Bartlett, 2015; Jaeger, 2015).

A point of special interest in the examination of Deep Web uses is related to digital libraries and databases with relevant sources that are not retrieved by the regular Web search engines but are nonetheless relevant for research in general (Kendrick, 2007; Theng et al., 2016). Addressing the challenges of navigating and collecting data in these environments, Pedley (2002) provides a distinction between the Surface and the Deep Web in terms of indexation and financial gains. The former is populated by commercial search engines that can make browsing easier, because they rely on private investment and profit, while the latter offers valuable open source content that should not be overlooked but equally is not that easy to find, since there is no institution making money from it. As noted by Su (2008, p. 74), the continuous innovation of digital platforms imposes challenges on researchers, and the Deep Web is an alternative to finding relevant content that could be forever lost, although this requires an extra effort: '[T]here are a number of reasons why one should expand searching to the Deep Web, as hidden below the surface is very useful and important information that may complement and supplement your research. This information may be unique, specialized, and authoritative.'

[10] Available on https://metrics.torproject.org/ Access: October 2019.
[11] Available on https://www.torproject.org/about/torusers.html.en Access: October 2019.
[12] Available on https://helpdesk.rsf.org/ Access: October 2019.

Looking back to the construction of the concept of the Deep Web, this part of the Internet was initially called the "Invisible Web" by Ellsworth & Ellsworth (1994) in an attempt to define the entire body of digital content outside of traditional platforms. In this metaphor related to visibility on the Internet, the proportion of content that is easily seen, i.e. accessible, is called the "Visible Web." Even now, the term "Invisible Web" is used by researchers such as Devine & Egger-Sider (2014), for whom the name has the same value as the Deep Web. As noted by Devine & Egger-Sider (2014, p. 3), the definition of this space is connected to 'all the rich and valuable resources not found by general-purpose search engines, including government information, journal articles, white papers, special collections of materials, blogs, wikis, social media.' A common criticism of the use of the term Invisible Web, however, is that it is inaccurate and generic, because it deems all non-indexed or badly indexed pages as simply invisible, when in fact they are actually visible and available but just need to be found through a different logic (Shestakov, 2008). The development of the term Deep Web was actually a consequence of the discontentment with the term Invisible Web. Bergman (2001, p. 2) argues that referring to this part of the Web as invisible is imprecise, since 'the only thing "invisible" about searchable databases is that they are not indexable nor able to be queried by conventional search engines.' According to Bergman (2001), this content is visible to those who need to access it. Therefore, the Deep Web is considered a better choice, generally defined by Bergman (2001) as a space where the Internet hides content from technology clusters and governments. Thus, another name commonly used by researchers is the "Hidden Web," which relies on the idea of hidden content, although 'the terms Hidden Web and Deep Web are generally interchangeable, and it is only a matter of preference which to choose' (Shestakov, 2008, p. 5). The discussion about meanings and concepts associated with the Deep Web technologies is presented in Chapter 4, entitled *Struggles of Meaning and Concepts: A Deep or Dark Web?* For now, it is possible to trace the evolution of this concept from the adjectives that have accompanied the Web through the time. It starts with an idea of invisibility that calls for non-existence (Ellsworth & Ellsworth, 1994), it then connects with the meaning of depth, which represents a larger potential area (Bergman, 2001), and finally adds the notions of non-indexable or hidden that appeal to a shady place (Shestakov, 2008).

From a technical angle, research about Deep Web systems in the field of Computer Sciences has produced extensive results commonly connected to cybersecurity, search engines and access to databases. It is the case, for instance, that Google researchers have worked on addressing the gap that the Deep Web presents to search engines and proposed an algorithm that forcefully indexes this hidden content, making it available on the Surface Web (Madhavan et al., 2008; 2009). In another example, Nunes et al. (2016) developed an operational system to gather information from multiple platforms, especially the Deep Web, as a proactive intelligence effort against cyber threats – especially terrorist attacks. Research also focuses on the Deep Web's general structure (Singh, 2002), discussions of the Deep Web as a possible Semantic Web (Wright, 2008), challenges with data extraction (Liu, Meng & Meng, 2010; Lu et al., 2007; Yamada, 2004), issues with search interfaces (Khare et al., 2010) and how to integrate them (Wu et al., 2004; 2006) and latent developments in new crawling techniques (He et al., 2013) among many others. It is worth mentioning here, however, that this thesis acknowledges technical issues and challenges, but the focus remains on how the British press represents its diverse social uses.

Finally, another concept that is relevant to this work is related to the Dark Web, but it is important to note that is not a synonym for the Deep Web: while the Deep Web is generally defined by Internet content not indexed by standard search engines (Bergman, 2001), the Dark Web (or the Dark Net) refers to criminal or antisocial uses of this segment of the Internet by people that apply anonymity for illegal purposes and to avoid legal persecution (Bartlett, 2015). In an additional distinction, according to Bradbury (2014, p. 14), 'the media is littered with discussions of the deep web and the dark web, but they are different entities.' The first is related to un-indexed content on the Web, and the second is an alternate layer 'often constructed by a community that wants to preserve anonymity, autonomy, or perhaps an ideology.' As one might deduce, the Deep Web contains and enables the Dark Web, but criminal use is only a part of the Deep Web. This chapter presents further explanations on this topic, but this initial clarification is necessary for the next section, which discusses Tor, the most widely known Deep Web technology.

2.6 The Onion Router

The Tor Network is the most popular Deep Web technology, considering that the Deep Web is mainly a collection of networks, websites and databases that require specific software or routines to gain access and are not simply available to everybody through traditional Web browsers (Sui et al., 2015). An abbreviation for the phrase "The Onion Router," because it applies multiple layers (as an onion) of encryption, Tor was developed by the Naval Research Laboratory of the United States to protect governmental communications and released in September 2002, but nowadays it is a non-profit organisation called The Tor Project (Bartlett, 2015). It is crucial to understand that Tor is one example of Deep Web technology, and whilst it is the most widely known example, it is obviously not the only one. Graham & Pitman (2018, p. 22), for instance, researched the specific case of another technology called Freenet as 'a wilderness, an anachronistic, barren digital space that supports anonymous self-expression and deviance. Freenet is in this way a singular Darknet space that should not be conflated with other Darknet spaces like Tor.' According to its own website[13], Tor is free software (a browser) and an open network that defends users against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and even relationships.

The key tool in Tor's operation is encryption. Considering that modern cryptography is a science related to the protection of data privacy through computer and communication security, encryption is one kind of cryptography based on protocols used to provide privacy over a secret key shared by the sender and the receiver, thus protecting the message (Bellare & Rogaway, 2005). With layers of encryption, Tor is a complex traffic system that makes the route between the user and accessed data untraceable (Dingledine et al., 2004). In fact, in the definition provided by Moore & Rid (2016, p. 15), and which includes Tor as the main example, '"Darknet," colloquially, refers to a distinct network supporting cryptographically hidden sites.' In terms of hardware, Tor is composed of a chain of relays: computers used to access content, routers provided by the network of volunteers and servers making content available. With Tor, computers provided by volunteers around the world compose a network of thousands of routers

[13] Available on https://2019.www.torproject.org/about/overview.html.en Access: October 2019.

that are randomly combined in circuits of three nodes, namely an entrance router, a middle router and an exit router, each of which is responsible for the decryption of one layer with an exclusive key, as Figure 3 exemplifies (McCoy et al., 2008).

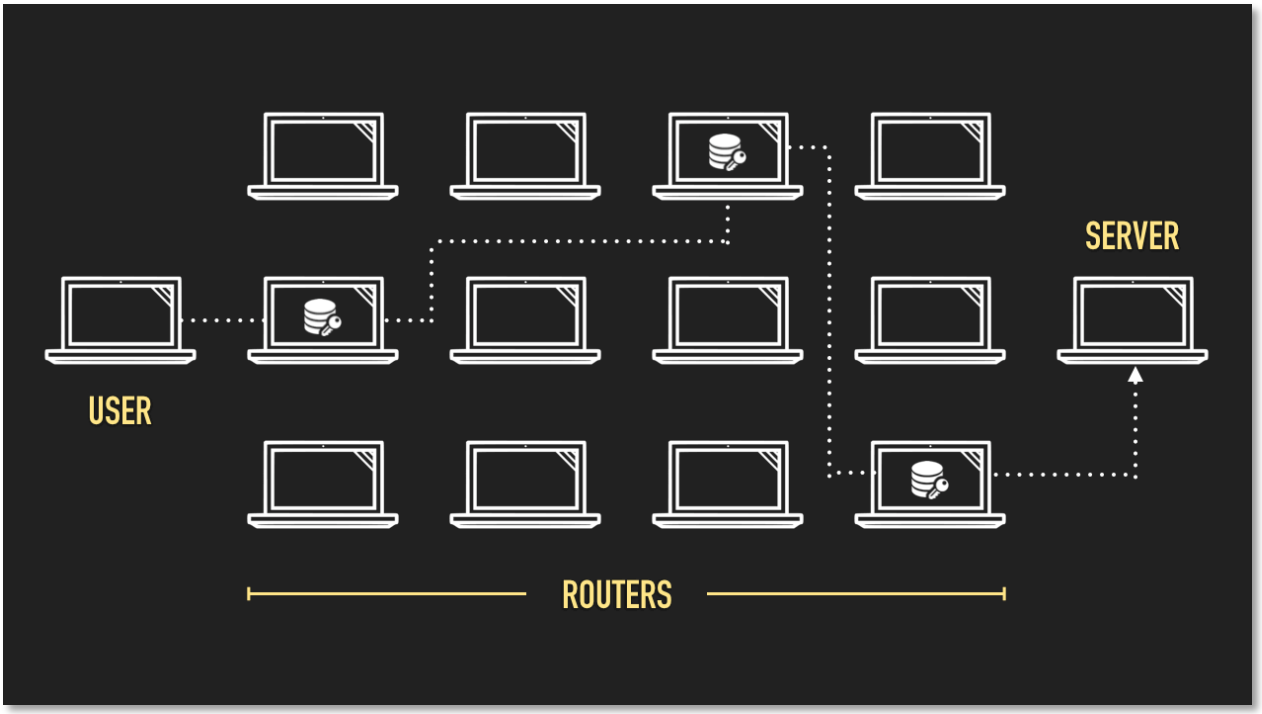


Figure 3: Sample of the Tor Network adding three layers of encryption between the user and server
Source: designed by the author

As noted by Reed et al. (1998, p. 487), 'to build the anonymous connection to the exit funnel, the onion proxy creates an onion. An onion is multi-layered data structure that encapsulates the route of the anonymous connection starting from the onion router for that exit funnel and working backward to the onion router at the entry funnel.' In the case of Tor, the entrance knows the origin of access (user's computer), and the exit recognises the content (website server), but a single node is unable to identify both the client IP address and the data. In fact, obfuscating geo-surveillance is a key reason for Tor's popularity (Doyle, 2018; Swanlund & Schuurman, 2019). Thus, it is a network essentially because of thousands of routers voluntarily provided by users, educational institutions and companies to ensure the existence of this privacy-enhancing software (Loesing, 2009). As a browser, Tor is unique compared to Internet Explorer, Google

Chrome and others, because it is the exclusive gateway to the Tor Network, in that accessing the network depends on the software. However, Tor works as any other Internet browser, so it can also be used to access the Surface Web.

In terms of infrastructure, Tor can be seen from at least three standpoints. From the historical perspective, it represents a sociotechnical system that was privately developed, and then used by others, to become part of a network or web of systems that would ensure the functionality one of the other (Plantin et al., 2016). From the sociological perspective, Tor is part of a community in which technical aspects evolve through social use, so the human element affects and changes the infrastructure, creating new practices and habits (Plantin et al., 2016). Finally, from the relational perspective, although infrastructure studies focus on the structural and technical aspects of technology, not the symbolic element, the human experience that evolves cannot be disregarded (Sandvig, 2013). Considering the material dimension of Tor, i.e. a digital system with physical and technical aspects, materiality is seen not only in the network of relays, but also in the digital signals such as applications used to run and control the systems and which are fundamental for the material realisation and the production of digital experiences (Dourish, 2015). In fact, Internet routing – not the Internet routers or the Internet route – is considered material, once 'it provides a way for data to move across multiple networks' (Dourish, 2015, p. 189).

Another point that makes Tor distinctive as software is that providing layers of encryption turns it into an anonymity-granting technology used to 'circumvent censorship, exercise a right to free expression and maintain their privacy in the face of an abusive regime (or even non-governmental vigilantes, trolls or bullies)' (Jardine, 2018a, p. 2). Baek, Seo & Kim (2016), for instance, propose software based on Tor technology as a way of providing anonymity and protecting patient information in a healthcare system. Although Tor can protect sensitive research and communication (van Baalen, 2018), Jardine (2018a, p. 4) argues that there are 'uses and abuses of the Tor network, as it is the most popular entry point into the Dark Web' – this specific discussion takes place further on in this literature review.

The privacy-granting aspect of Tor is directly related to the Onion Service Protocols, which have been available since 2004 and are also known as "Tor Hidden Service Protocols": 'Onion

services are services that can only be accessed over Tor. Running an onion service gives your users all the security of HTTPS with the added privacy benefits of Tor Browser.'[14] Basically, Tor provides the option for web developers to create websites using their protocol, which means a .onion website, as a way of ensuring more protection in interactive applications such as web browsing, file-sharing and instant messaging. In general, creating a .onion address is a way of keeping a webpage safe from web crawlers, tracking and surveillance. In fact, The Tor Project won the Free Software Foundation Award for Project of Social Benefit in 2011[15], exactly for enabling millions of people around the world to access the Internet with freedom. Among other things, Onion Services offer location hiding, end-to-end authentication, end-to-end encryption and network address translation (NAT) punching. Therefore, an Onion Service[16] relies on development and access to ensure privacy. All .onion websites can only be accessed through Tor; however, services such as Tor2Web[17] work like a proxy, creating a new address for .onion pages and making them accessible from regular browsers, albeit these browsers cannot assure the user's anonymity, in the same way Tor manages to do. It is worth mentioning here that 'most Tor users have never visited any hidden website at a *.onion address; hidden services account for around 3–6% of overall Tor traffic. Most users instead use the software merely to browse the internet's conventional address space more securely or anonymously' (Moore & Rid, 2016, p. 16).

Onion Services can be used in positive or negative ways. On the one hand, these protocols can help protect freedom of speech, since 'it [is] possible to establish a connection to a source that leaves no trails for most authorities. Rather than seeing technology as a threat overall to journalism and sources, it makes more sense to think of the digital landscape as a new battleground in which innovative, often rapidly changing rules apply' (Grey, 2016, p. 61). The most famous contemporary whistle-blowing website, WikiLeaks, is one such example, because although there is a website on the Surface Web[18], when the user clicks on the 'Submit' button,

[14] Available on https://community.torproject.org/onion-services/ Access: October 2019.
[15] Available on https://www.fsf.org/news/2010-free-software-awards-announced Access: October 2019.
[16] Available on https://2019.www.torproject.org/docs/onion-services Access: October 2019.
[17] Available on https://www.tor2web.org/ Access: October 2019.
[18] Available on https://wikileaks.org/ Access: October 2019.

which means that the person is about to share sensitive content or a secret document, this user is forwarded to a .onion address to do it safely (see Figure 4). As noted by Moore & Rid (2016, p. 16), 'anonymous browsing is not part of the "dark web"; it is a legitimate and laudable service that Tor provides.' Moreover, Tor has a strong social, economic and political impact, according to Cammaerts (2013, p. 420), as 'WikiLeaks evolved from a faceless intermediary enabling whistleblowers to publish documents while remaining anonymous to being an active actor, selecting/reacting material and reaching out to mainstream media to increase exposure.'

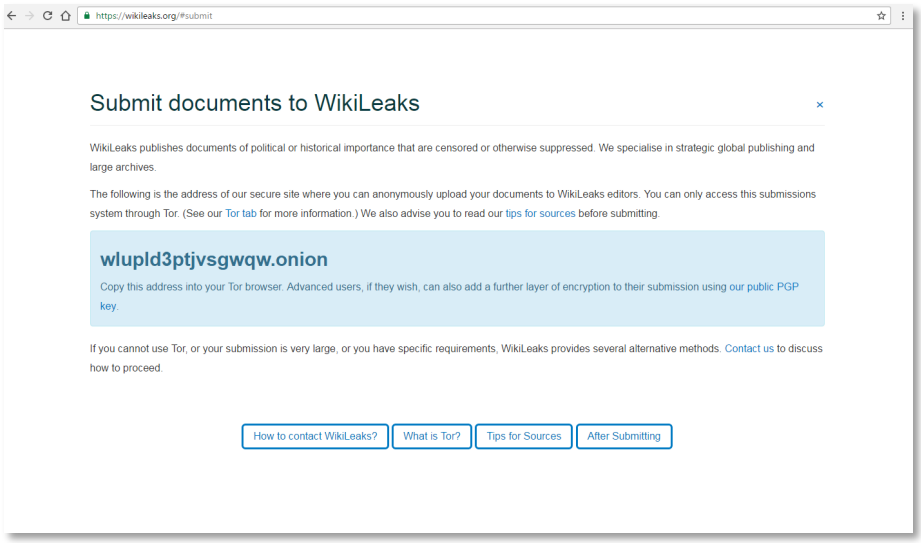


Figure 4: WikiLeaks submission webpage
Source: https://wikileaks.org/wiki/WikiLeaks:Submissions#submit
Retrieved by the author in October 2019

Another positive use is related to access to information. In October 2019, the British Broadcasting Corporation (BBC) released a .onion version of their website, providing the following explanation: '[T]he BBC has made its international news website available via the Tor network, in a bid to thwart censorship attempts. The Tor browser is privacy-focused software used to access the dark web. The browser can obscure who is using it and what data is being accessed, which can help people avoid government surveillance and censorship. Countries including China, Iran and Vietnam are among those who have tried to block access to the BBC

News website or programmes.'[19] As part of the official statement, the corporation argues that 'the BBC World Service's news content is now available on the Tor network to audiences who live in countries where BBC News is being blocked or restricted. This is in line with the BBC World Service mission to provide trusted news around the world.'

In summary, Tor combines a browser and a system of thousands of relays maintained by a voluntary network that provide privacy and a gateway to services developed globally, with the aim of protecting people's privacy in a way that does not happen with the Surface Web. However, there is a latent discussion regarding Tor protecting the anonymity of criminals. Kane (2015, p. 1), for instance, argues that it should have a 'system that will ensure anonymity for all its users, while maintaining the ability to break the anonymity of a sender in case of misconduct.' The issue with this approach is determining who would decide about what does or does not constitute misconduct. If this power is given to the state, for instance, what happens to people that use Tor to protect themselves in highly repressive regimes? As a result, the Tor Network is a complex community that feeds itself with infrastructure and content and, thereafter, an example of the possibilities of the Deep Web. It is worth mentioning here that this research acknowledges the negative uses of Tor. Providing anonymity and safe access to users everywhere, Onion Services enable an environment in which policing action and legal persecution are limited, so crimes are less likely to be punished. It is clear that Tor facilitates crimes such as illegal trade on the crypto markets (Baker, 2015; Mackey, 2018; Martin, 2014; Negri, 2016; Smirnova & Holt, 2017), child exploitation networks and the distribution of paedophilia material (Bleakley, 2019), terrorist and far-right movements and organisations (Abbasi & Chen, 2007; Al-Rawi, 2019; Chen et al. 2008; Greenberg, 2016; Hossain, 2015; Qin et al., 2005; Weimann, 2016a; 2016b) the trade of stolen data (Smirnova & Holt, 2017) and others. The next section focuses on the abuses of these technologies, which turn the Deep into the Dark Web.

[19] More on https://www.bbc.co.uk/news/technology-50150981 Access: October 2019.

2.7 The Dark Web

As noted by Hawkins (2016), there is a certain amount of ambivalence in regard to the Deep Web's uses: virtual academic libraries, safe email services and digital repositories on the one hand, and illegitimate and illegal business on the other hand. Bartlett (2015, p. 3) argues that the distinction between the Deep and the Dark Web relies on usage, in that the Dark Net – a term adopted by the author – is 'an underworld set apart yet connected to the Internet we inhabit, a world of complete freedom and anonymity, and where users say and do what they like, uncensored, unregulated, and outside of society's norms.' Nevertheless according to Bartlett (2015), the Dark Net is a space without limits or censorship that provides a huge chance to explore curiosity and desire, where the boundaries can be pushed, any idea can be expressed and freedom is used for crimes. Besides that, Bartlett's (2015) conceptualisation considers that the Dark Web is related not only to the Deep Web, but also to criminal or antisocial activities on the Surface Web, such as spam, cases of cyberbullying and online scams. As noted by Gehl & McKelvey (2019, p. 223), in this context, 'the adjective "dark" may bring to mind illegal or immoral activity.' Moreover, Gehl & McKelvey (2019, p. 223) provide a specific definition: '[D]arknet, however, emphasizes its technical aspects, focusing instead on access, protocols, encryption, and network topologies. In this sense, our definition is more akin to "going dark" in communications.' Although this research acknowledges this compelling argument, the focus of this thesis is specifically on the representation of Deep Web technologies, and so the Dark Web is associated here with criminal and antisocial behaviours observed on the Deep Web, or more specifically Tor.

In relation to Tor's scope, Figure 5 assists in understanding the different parts of the Web, to which the Tor Network provides access. Considering the metaphor of the iceberg again, to explain the Web, content above the waterline is the Surface Web, and any content not accessible through the usual browsers is the Deep Web. This figure, however, adds the Dark Web to the picture, a space deeper and far more obscure, related to shadier practices. Finally, Tor is represented as the onion that can access all three spaces: as a browser to access content on the Surface Web, to gives access to .onion websites, which are part of the Deep Web, and the privacy and anonymity provided by Tor that enables the illegal activities that characterise the Dark Web.

Figure 5: Structure of the Web and kinds of content accessed through the Tor Network
Source: designed by the author

Negative uses of the Internet are seen as bugs, a drawback to technology's full potential, 'a sort of parasite to these large-scale media objects: darknets. These hidden, often anonymous networks attach themselves and then re-purpose infrastructures and platforms' (Gehl & McKelvey, 2019, p. 220). Considering the potential misuses of the Deep Web as the Dark Web per se, these technologies are seen as a hideout for online criminals, an environment in which they can freely conduct illegal activities beyond the knowledge of law enforcement, police and intelligence agencies. Omand (2015) argues that although these technologies were developed to protect people's privacy, they promote a change in relation to criminal actions, a whole new kind of criminality in which cyber-attacks replace shotguns, and criminals can be anywhere as long as they have a computer and Internet access.

As a space in which anonymity can be used to protect military communications as well as to plan terrorist attacks, Onion Services have led to the emergence of an ethical discussion. On the one hand, Tor enables anonymity that protects vulnerable groups and stigmatised communities (Barratt & Maddox, 2016), and it provides alternatives to social networking websites (Gehl, 2015),

thousands of digital repositories (Su, 2008), safe communications (Loesing, 2009) and ways of effecting civil rights resistance (Jardine, 2018a). On the other hand, the online underworld is a virtual no man's land whose benefits can be seen as not outweighing the losses (Omand, 2015). There are, of course, distinct levels of illegality on the Dark Web. Baker (2015, p. 120), for instance, highlights the use of crypto markets such as Silk Road to gain access to sensitive or even banned books: '[H]ere, every book you can imagine (and many you can't) has been uploaded and readers can browse anonymously,' which is different to selling drugs, which is also different to plotting terrorist attacks. Massanari (2017) argues, however, that the lack of accountability and the anonymity provided by Dark Web technologies can encourage and normalise toxic techno-cultures connected to undesirable online behaviours related to publishing and spreading offensive content, such as anti-feminist activism.

A negative use largely connected with the Dark Web is commerce in drugs, guns and other goods on crypto markets, with the special case of the Silk Road – although this example is focused on drugs, since weapons were earlier removed from listings (Lorenzo-Dus & Di Cristofaro, 2018). Launched in 2011, Silk Road is a pioneer among crypto markets, as Ferguson (2017, p. 683) summarises: '[L]ocated on the darknet, accessed via the Tor browser, Silk Road was the first of a new breed of darknet marketplaces and smartphone app-based drug markets. Participants on these transact under closely guarded aliases using sophisticated encryption.' Another case is AlphaBay (Tzanetakis, 2018), one of the largest crypto markets in operation nowadays and an analysis of which shows that these markets are regional, not global, and that their use is mainly via Western industrialised countries. The proliferation of innovative crypto markets promotes the sophistication of the drugs market, and it is noteworthy that crypto markets are defined as being 'hosted on the hidden or darknet, a subsection of the Internet where all communications are encrypted and anonymized, thereby protecting both the infrastructure hosting the marketplaces and identity of their users' (Demant et al., 2018, p. 256). As noted by van Hardeveld et al. (2017), cybercriminals employ multiple tools to trade securely for many years, but what makes Tor popular is that it provides a combination of anonymisation, peer-to-peer software (connecting buyers and sellers) and decentralised or distributed initiatives. Also with a negative view of the dissemination of cryptocurrencies and decentralised marketplaces, Pesch & Ishmaev

(2019, p. 271) state that 'these tools and instruments can bring about new forms of negative market externalities, such as the propagation of markets for illegal goods and services following the so-called "darknet markets" paradigm (hosted on the TOR network).'

According to Martin (2014, p. 352), Silk Road and other crypto markets influence the ways in which authorities deal with crimes related to drugs, because 'changes associated with online drug distribution signal a potential paradigm shift in the global War on Drugs, as costly and ineffective prohibition strategies are placed under further stress, and new, more efficient distribution networks form between drug producers and consumers.' Maddox et al. (2015) argue on the notion of constructive activism and see practices in the Silk Road community as a group of people against drug prohibition and who use this crypto market to stick to their beliefs but do not intend to change actual politics. Addressing the role of the Web in the commerce of false medications, Negri (2016, p. 357) states that 'organised criminal groups have taken advantage of modern communication strategies, and using the web – including the Darknet – has proved to be a safe and easy way to advertise and supply their dangerous products directly to patients and consumers.'

In terms of drugs consumption and legality, Seddon (2019, p 11) uses a constitutive approach to a necessary drug law reform, considering that 'if we take the example of online "darknet" drug markets, some policymakers have attempted simply to translate traditional drug prohibition approaches for the new problem,' which happens because of solutions that do not recognise all participants in the regulatory space, such as 'Internet service providers, website administrators, vendors, purchasers, other members of online communities, law enforcement agents (online and offline), transport services, customs officials, mail delivery services, home insurers and so on.' Considering that Dark Net market systems are generally vulnerable (Lane et al., 2018; Moeller et al., 2017), Salmon et al. (2019, p. 458) attribute to the technical challenges the fact that these spaces are not better policed, and instead they propose an option to "disrupt illicit marketplaces": 'the dark net continues to grow, and there is a need to explore the development of interventions designed to disrupt illicit activities.' Lorenzo-Dus & Di Cristofaro (2018), however, discuss ideas of trust and community in the Silk Road context, as well as policymaking attitudes regards crypto markets, to conclude that law enforcement actions against these

websites result in more technological innovation, and therefore it encourages the development of new tools to maintain activity.

In relation to discursive practices in crypto markets and forums on the Dark Web, Ferguson (2017, p. 694) presents the results of a four-year digital ethnography and concludes that there is a 'standard lack of consistency in grammar, spelling, and terminology, but participants are in fact making a concerted effort to not use certain terms, or not to use (or only to use) them in certain ways.' Besides, Ferguson (2017, p. 694) argues that 'there are cultural dynamics at play in the online environment in which participants are global, do not have a standard terminology or even a standard cultural context by which to frame their self-presentation and participation in these marketplaces.' Moreover, Ladegaard (2018, p. 241) argues that free drug samples are strategically used as a way to construct a community and attract users with the purpose of 'rak[ing] up reviews, cultivat[ing] customers, and increas[ing] trade.' From the socialisation viewpoint, Bancroft, Squirrell, Zaunseder & Rafanell (2019, p. 2) assure that navigating through these websites, and the Dark Web in general, requires cultural competence, as 'relationships conducted online present a challenge for maintaining trust. Trustful actors can be impersonated and trust signals faked to little cost for the malicious actor. That is particularly important for online illicit market exchanges, where there is a strong incentive to falsify and where the cost of doing so is low and the sanctions limited.' Moreover, 'trust is a key concern in the hidden net; those behind the creation and/or administration of crypto-(drug) markets are known to go to considerable lengths to show that members can trust that transactions therein are "safe," that is, there is a low risk of being caught by law enforcement and of being scammed by other members' (Lorenzo-Dus & Di Cristofaro, 2018, p. 609).

Nevertheless, research based in multiple countries suggests that drugs are traded on the Internet in general, and not exclusively in crypto markets. Discussing the specific case of opioids in the United States, Mackey (2018) argues that it is misleading to attribute the drug trade only to the Dark Web, as there are relevant websites on the Surface Web with the same purpose, as well as sellers that use social media channels to advertise their products. Rothberg & Stith (2018) focus on the issue of fentanyl as a central piece in the current epidemic and increase in deaths in the United States; however, they also note that the Dark Web is part of the problem, but not the

only source for these drugs. Décary-Hétu, Mousseau & Vidal (2018) analysed how practices of herbal cannabis drug-dealing changed in the United States over a period of six years on crypto markets – and the conclusion is that a small proportion of dealers and users actually adopted the online trade due to higher prices, lack of technical skills and unequal digital inclusion. Antonopoulos & Hall (2016, p. 706) looked at the consumption of anabolic-androgenic steroids in the United Kingdom to conclude that the Dark Web sites are only part of online sellers' toolset, which include 'OPs (*online pharmacies*), social media sites, forums, classified advertising sites.' Considering the case of China, research on the trade in psychoactive substances determines that 'although the Internet was involved in the domestic supply chain and had become fully embedded within the whole process of smuggling, however, the role of the darknet is still unknown' (Zhao, 2019, p. 18). It is not only the case for drugs, though. Through researching hacker socialisation, Dupont et al. (2017) unveiled that the Darkode, the most prominent and exclusive forum for highly specialised users seeking to trade malicious software as well as stolen data, existed for years on the Surface Web.

Aldridge & Décary-Hétu (2014) analysed the nature of trade on Silk Road to argue that the website cannot be considered 'eBay for drugs,' as often claimed by the media, because most transactions are business-to-business, and therefore between major and minor dealers (local street operators), creating a new breed of retail drug dealer using technology and large stockholdings to control the industry. Nevertheless, according to Aldridge & Décary-Hétu (2014), this new way of trading drugs could reduce violence, intimidation and territorialism in the context of the drug industry. Bakken, Moeller & Sandberg (2018) even suggest that these markets are more efficient than the traditional ones, in that they not only reduce visibility and violence, but they also offer competition and cooperation. From a different perspective, and considering that not only illicit substances but also other goods can be commercialised in crypto markets, Oliveira, Natarajan & da Silva (2019) affirm that they can influence criminality on the streets in other ways. According to Oliveira et al. (2019), anonymity provided by the Dark Web enables thieves to easily and safely sell good stolen in bus robberies, which is a common crime in most developing countries. This includes trade in second-hand watches, jewels, smartphones and other products.

Terrorist groups and far-right movements are also amongst the most feared users of the Dark Web. Research on this matter started quite early. Qin et al. (2005), for instance, developed a system to analyse content and understand the extent of the terror discourse on the Dark Web, while Weimann (2016a; 2016b) points out the technological sophistication of these groups, and Bartlett (2015) acknowledges that a common reason why privacy-enhancing technologies are distrusted is exactly because they can make terrorists and other radicals untraceable. According to Hossain (2015, p. 142), the fact that these groups use Tor shows that 'the terrorist organisations are tampering the Internet platforms including the social media platform in order to communicate for their terror activities to other members of the group.' Al-Rawi (2019, p. 235) argues that audio-visual materials play a relevant role in Islamic State (ISIS) propaganda, especially to 'provide a standardized social media literacy crash course on whom to follow, block, and how to retweet as well as the importance of protecting ones online privacy using the Dark Web (Tor network) and VPNs.' Besides, analysis of North-American supremacist and Middle-Eastern extremist forums shows that the use of violence and hate in the discourse is robust, albeit even stronger in the case of the latter (Abbasi & Chen, 2007); therefore, developing an efficient Dark Web crawling system would enhance authorities' knowledge of these groups (Fu, Abbasi & Chen, 2010). Indeed, as noted by Chen et al. (2008), extracting data from the Dark Web plays a relevant role in guiding policymaking and intelligence action against the Jihad. From an additional perspective, Greenberg (2016, p. 176) discusses the more positive side of the Dark Web being used by terrorist groups such as ISIS for both propaganda and recruitment: '[D]riving ISIS to use the dark web can be a worthwhile outcome. Getting ISIS off of popular platforms diminishes their reach and their effectiveness. It is akin to pushing them into a cave […] The dark web forces ISIS into the shadows, making it more difficult for American citizens to start down the extremist rabbit hole.'

Another special point is related to child exploitation networks and the distribution of paedophilia material. As argued by Bleakley (2019, p. 221), global criminal networks are beneficiaries of the digital age, as it helps to establish connections: '[T]ransgressions continue to take place in the digital realm in the form of consuming and sharing child pornography; on some occasions, Dark Web forums can also facilitate transgression in the physical realm, by making

connections between consumers and producers of exploitation material, providing an opportunity for consumers to transition into participation in the production of illicit material.' The trade in stolen data is also an issue, both on the Surface and the Dark Web, depending on the sophistication of policing strategies against cybercrime (Smirnova & Holt, 2017, p. 1409): '[T]o further avoid the likelihood of detection, sellers could move their advertisements to Tor-based forums and shops. Tor services minimize the ability for actor attribution, which may enable sellers to operate with greater impunity to sell data from all countries.' Mörch et al. (2018) discuss searches and forums related to suicide and the extent to which Tor is used by people investigating the topic, generally or looking for methods. They conclude that the Surface Web offers much more content on the topic than Tor, although content on the Dark Web is more pro-suicide, which indicates the need to devise specific strategies to prevent suicide in these environments.

From an economic point of view, the Dark Web is commonly connected to the discussion about cryptocurrencies, such as Bitcoin, which are used to enable illegal trade or sponsor criminal activities that assist drug dealers and extortionists (Kethineni & Cao, 2019). Furthermore, Ladegaard (2019) applies the 'darknet economy' concept to the association between three technologies that allow for free commerce on the Internet: Tor, crypto markets and Bitcoin. Bjerg (2016, p. 53) defines Bitcoin as 'a peer-to-peer electronic payment system that operates as an independent currency,' whilst Kang, Choo & Kim (2019, p. 2) argue that 'Bitcoin markets are now often recognized as sites for speculators' as well as fraud activities. According to Brown (2016, p. 328), although a cryptocurrency is not inherently criminal, 'the lack of independent regulation and the possibility of evading the anti-money laundering principle of "know-your-customer" have created both additional and attractive opportunities for criminal exploitation.' In the same way, Kavanagh, Miscione & Ennis (2019) connect digital money to illegal activities and the Darknet while discussing the social constructs related to money and how cryptocurrencies such as Bitcoin play a part in this game. On the challenges that crypto currencies impose from a regulatory perspective, Latimer & Duffy (2019, p. 129) connect Bitcoin to criminals and hackers, to whom 'digital currency provides an online medium of exchange to buy, sell and trade illegal goods and services on shared networks on the darknet such as drugs, weapons and child pornography.' As noted by Ducas & Wilner (2017, p. 555), however, it is clear that the 'association between

cryptocurrencies and illegal activities is further augmented by the exclusive use of these currencies across illegal online services and marketplaces accessed through an encrypted layer of the Internet, the so-called "dark net".'

In summary, through examples of crimes against children, the financial system, general public health and even mankind, this section shows multiple ways in which Deep Web technologies can be misused and, as the Dark Web (Bartlett, 2015), cause harm on personal, social, national and global levels. While it is relevant to consider these discussions, to put the Dark Web into perspective, the focus of this research is not on the activities that happen in this space but actually how the British press represents these technologies, as well as their uses and users.

2.8 Tor 101

Having examined key concepts and phenomena related to the Deep Web, it is useful to take the perspective of a hypothetical Deep Web user and establish how a person can access resources that are otherwise not available on the Surface Web. This section aims to underline briefly the steps that a user is advised to follow, to assure private and anonymous access to the Internet with Tor, according to its website[20]. The widespread unease about the impact of the Internet on privacy and surveillance suggests that the use of such tools might concern in the future more than a small potential category of expert users and hackers. Research conducted by the Information Commissioner's Office (2019) about trust and confidence in companies and organisations that store and use personal data shows an overall pessimist picture: 38% of the people have low trust and confidence in these institutions. Considering these numbers, and the notion that Tor is a technical option for online data protection, this section aims to demystify the use of this technology. This includes a four-step path (see Figure 6), namely a virtual private network (VPN), the Tails operating system, the Tor Network and Onion Services –, a combination that provides an efficient level of privacy, according to The Tor Project.

[20] Available on https://tb-manual.torproject.org/ Access: October 2019.

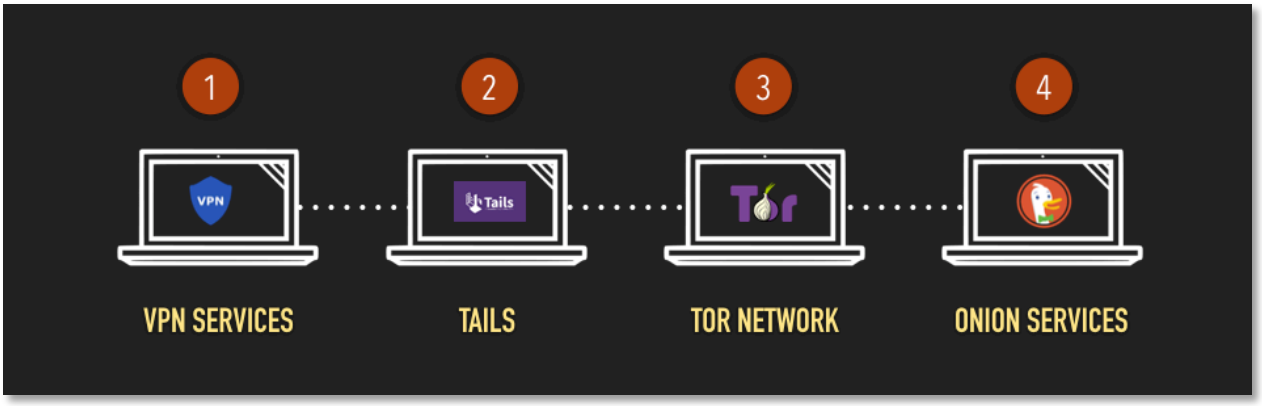


Figure 6: Four steps for private access to the Deep Web
Source: designed by the author

The first step is to contract a VPN service, which is basically an application that offers distinct locations around the world for the user to choose from and automatically changes the original computer's IP address for another one in the chosen location (Bartlett & Krasodomski-Jones, 2015). This service is available through paid and free options, although the paid versions are considered more reliable and offer more functionalities, which can be downloaded onto computers, smartphones or tablets. Using a VPN service assures that if the IP address is found, in the event that the access is somehow tracked, it does not lead to the user's original computer. In fact, the user can access websites such as myIPaddress.com[21] to be sure that the IP address has changed – even Google provides the IP address if the person searches for "google check IP address" or something similar. As noted by Hoang & Pishva (2014), data are protected on two distinct levels with a VPN service. First, users' data are automatically encrypted when the device is connected to a VPN and data exchanges are made through secure tunnels. However, services that keep the information on their servers are vulnerable to breaches, since personal data can be leaked if 'a VPN server gets hacked, controlled by an organisation that makes business out of users' private information or make them available to government entity upon request' (Hoang & Pishva, 2014, p. 38).

[21] Available on http://www.myipaddress.com/what-is-my-ip-address/ Access: October 2019.

The second step is related to the Tails operating system, a free and open software suite that presents itself as 'the amnesic incognito live system'[22]: amnesic because of its short-term memory, and incognito because it protects people's identity. According to its own website, Tails helps people to 'use the Internet anonymously and circumvent censorship; […] leave no trace on the computer you are using unless you ask it explicitly; use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.' The key point that makes Tails different from other systems is that it can be installed on a DVD, a USB stick or an SD card. When the user connects the external drive to a machine, Tails works independently of the original operating system – such as Windows or Mac OS – and at the end of the browsing, when the user disconnects the external drive, it automatically deletes the history. As this online activity is not registered by the original operating system, all details about this access are permanently lost.

These two previous steps – activating a VPN service and using Tails – are the forerunners to gaining access to the Tor Network. It is worth mentioning here that Tails was developed to be used in combination with Tor, as according to Tor's website 'all software is configured to connect to the Internet through Tor; if an application tries to connect to the Internet directly, the connection is automatically blocked for security.'[23] Therefore, there is an association between Tor and Tails. The third step involves downloading and using Tor. The software can be downloaded at The Tor Project website,[24] and although it works as a gateway to a network made up of thousands of voluntary routers that create a complex system of encryption, its appearance and functionalities are exactly like any other web browser, as Figure 7 shows. In addition, Figure 8 shows how a circuit of connections is made when using the network – which includes an option to move to a new circuit.

[22] Available on https://tails.boum.org/ Access: October 2019.
[23] Available on https://tails.boum.org/about/index.en.html Access: October 2019.
[24] Available on https://www.torproject.org/download/ Access: October 2019.

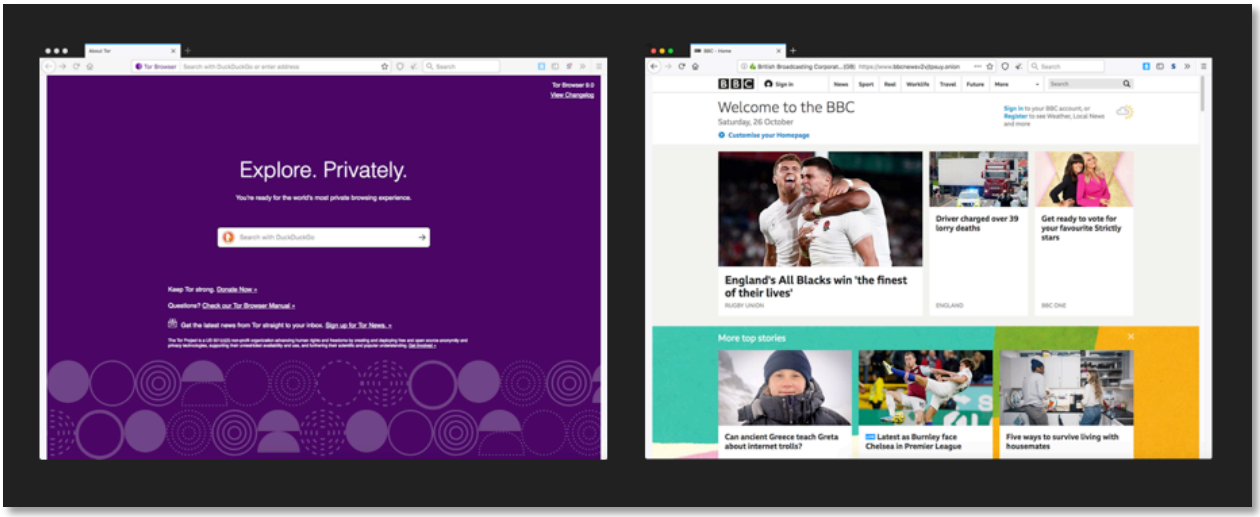


Figure 7: Examples of browsing with the Tor Network
Source: the Tor Network
Retrieved by the author in October 2019

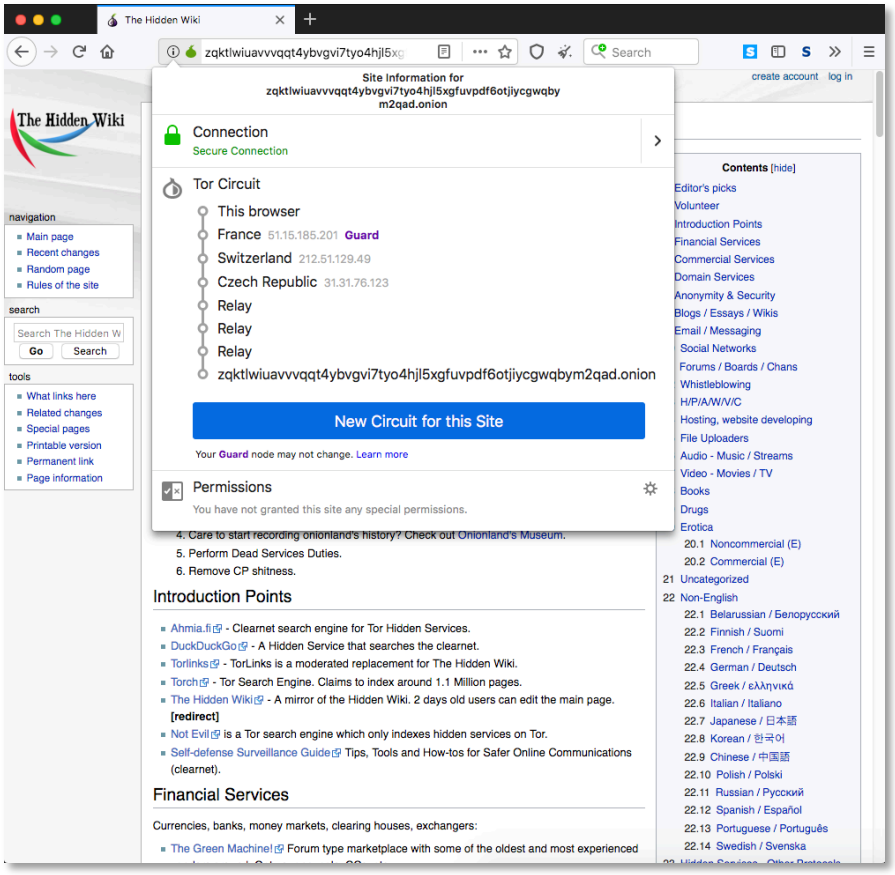


Figure 8: Example of a connection using the Tor Network
Source: The Hidden Wiki
Retrieved by the author in October 2019

It is important to highlight that Tor provides a higher level of privacy when people access websites developed through the Onion Services, and which are therefore made to protect users' personal data. If a user takes all three previous steps but then accesses Facebook or Gmail with their usual login, this person can be identified. Thus, the fourth step is related to these services: this protocol for secure access is only complete if the user is accessing an Onion Service, for instance DuckDuckGo[25], 'the search engine that doesn't track you,' according to its own webpage. Another useful website is The Hidden Wiki[26], which is a portal of links for other services. Onion

[25] Available on 3g2upl4pq6kufc4m.onion Access: October 2019.
[26] Available on http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page Access: October 2019.

Services also offer hundreds of forums, book repositories, instant messaging services, email providers and crypto markets, as mentioned before. In summary, the pathway to obtaining anonymity starts by changing an IP address through a VPN service, moving on to using the Tails operating system, to avoid keeping access history, then using Tor and, finally, accessing Onion Services.

2.9 Conclusion and further Contributions

This chapter presents relevant literature on the topic of the Deep Web, which is the focus of the empirical research that follows. This requires an understanding of the Web developed as a space in which information could travel and exist (Berners-Lee, 2000) and which over time became an interactive setting for communication and data exchange (O'Reilly, 2007), thereby enabling a network economy (Barabási, 2002), a network society (Castells, 2010) and a culture of connectivity (Van Dijck, 2013). The issue is that while offering benefits that facilitate everyday tasks, digital technologies collect data about users' behaviour (Lyon, 2009; 2018) through surveillance practices encouraged by state and private companies (Dinev et al., 2008), thus creating a powerful network of information which is a main risk to privacy (Gray, 2003) and promotes inequalities (Gandy, 1993). Pursuing online privacy, in this sense, is a response to digital surveillance (Lippert & Walby, 2016) and a way of protecting society (Nissenbaum, 2010). Moreover, online anonymity is defined by social uses and understandings, i.e. reducing the dangers of the Web (Hoang & Pishva, 2014), facilitating discussions about sensitive topics (McLeod, 2011; Sharon & John, 2018; Wu & Atkin, 2018), empowering people in highly repressive or highly liberal contexts (Jardine, 2018b) and imposing a limit to surveillance logic (Floridi, 2014), among other uses. Privacy-enhancing technologies such as Tor enable online anonymity and are responsible not only for the positive uses previously mentioned, but also for creating new and more efficient forms of cybercrime (van Hardeveld et al., 2017), crypto markets (Martin, 2014; Morselli et al., 2017), hacking technology sophistication (Hoang and Pishva, 2014), illegal file-sharing (Larsson et al., 2012) and so on.

Surveillance practices, privacy issues and discussions about uses for online anonymity are part of the reason why the Web can be separated into three parts, as this thesis argues: the

Surface, the Deep and the Dark Web. The Surface Web is populated by content used by search engines and aggregated by crawlers, which are responsible for indexing, web archiving, data mining and monitoring services (Olston & Najork, 2010). Any content that is not indexed, and therefore not found by Internet crawlers, is called the Deep Web (Bergman, 2001), including valuable and diverse resources (Devine & Egger-Sider, 2014). Finally, the Dark Web refers to criminal or antisocial uses of Deep Web systems by people who apply anonymity for illegal purposes and to avoid legal persecution (Bartlett, 2015). This research focuses on the British press representation of the Deep and the Dark Web as well as the Tor Network, a Deep Web technology that uses encryption to protect Web browsing by providing online anonymity (Bellare & Rogaway, 2005; Dingledine et al., 2004; McCoy et al., 2008; Moore & Rid, 2016) and obfuscating geo-surveillance (Doyle, 2018; Swanlund & Schuurman, 2019).

Criminal uses of these technologies are one of the reasons why they are feared, but this research does not focus on the criminal activities that happen in this space; instead, it unveils how the British press represents these technologies and what associations are made as a result. Although Gehl (2016) states that 'most journalistic work on the dark web presents it as composed of illicit activities in need of policing,' more empirical research is still lacking which provides evidence for this claim and which also enables more sophisticated analysis and contextualisation of the patterns of representation and perceptions surrounding the Deep Web. This thesis fills this gap by providing empirical research to corroborate widespread preoccupations about the demonisation of Deep Web-related technologies and by deepening insights into how technologies, activities and users of the Deep Web are portrayed by the media – and specifically by the press.

3 Methodological Framework

Considering the discussions about online privacy, as well as technical and sociological aspects of the Deep Web and the Tor Network, as addressed in the literature review, this research aims at understanding how the British press represents these technologies in terms of meanings, uses and users. Consequently, this thesis relies on an extensive empirical research of 833 newspaper articles examined through two methods: content analysis and critical discourse analysis. As noted by Deacon et al. (2007), and argued in the next sections, mixed methods followed by academic rigour assures eclecticism and strength for the research, from data collection to analysis. Besides, in order to present a clear structure and understanding, this chapter is organised into three main parts. The first introduces the overall research, such as the research problem, objectives and questions. The second part focuses on data collection and analysis, including the sample, methods and challenges, and finally, the third part is related to the ethical discussion.

3.1 Research Problem

This research centres on the British press representation of the Deep Web and the Tor Network, considering not only the approach to their technical perspective, but also hopes and fears related to their meanings, uses and users. This entails initially unveiling how the imaginary of the Deep Web is constructed in the newspapers' daily coverage concerning concepts, definitions and meanings. Thereafter, this research presents analysis and discussions related to how these technologies, especially the Tor Network, are framed by the media, with associations that vary from the negative connotation of criminal and antisocial behaviours to the optimism of a liberation technology.

3.2 Research Objectives

The main objective of this research is to understand the British press's representation of the Deep Web and the Tor Network. Considering this general aim, there are four specific objectives:

1. To examine how the British press present concepts and meanings of the Deep Web.
2. To comprehend how the press portray the uses and users of the Deep Web.

3. To unveil UK newspapers' discourse on the Tor Network.
4. To position the Deep Web's media representation in the general imaginary of the Web.

3.3 Research Questions

Considering the main and specific objectives mentioned above, this study proposes to answer to the following research questions (RQ):

RQ1) How do the British press represent the Deep Web?

RQ2) What discourse do the British press use to portray the Tor Network?

RQ3) To what extent does the British press's representation of the Deep Web technologies influence the overall imaginary of new media and the Web?

3.4 Research Sample

This research focuses on the analysis of newspaper content as a way of understanding the British press's representation of Deep Web technologies. It is worth mentioning here that the print media in general, and specifically newspapers, are a relevant source of information for adults in the context of the United Kingdom, as noted by the report *News Consumption in the UK: 2019*, recently published by The Office of Communications (Ofcom). This report shows that although the circulation of national newspapers has been decreasing lately – from nearly 22 million in 2010 to 10.4 million in 2018 –, 49% of the respondents mention newspapers (printed or via websites and apps) as their main source of information. Furthermore, 11% of them seek newspapers specifically for in-depth analysis, and there is a predilection for tabloid newspapers, with 30% of them choosing *Daily Mail* as their preferred title (Ofcom, 2019).

Considering this scenario, and also that, as argued by Chadwick, Vaccari & O'Loughlin (2018, p. 427), British newspapers are generally divided between tabloid and quality, and tabloids are the ones 'significant in the diffusion of misinformation and disinformation,' this research mixes quality and tabloid titles in the analysis, in order to pursue a more accurate view of the British print media. According to Thurlow (2006, p. 687), it is a privilege to conduct a study including multiple titles, as 'it offers an otherwise unique opportunity to see how a single issue is reported in many different papers, from many different locations, and over a substantial period. This in

turn puts the researcher in a better position to identify structural patterns, topical consistencies emergent cultural narratives.' Finally, the selection of newspapers for this analysis, as Table 1 highlights, considers three main points to assure the representativeness of the sample and a broader scenario of the UK print media: daily reach (PAMCo, 2019), political affiliation (Wring & Deacon, 2010) and nature (tabloid or quality).

Table 1: UK newspapers by political affiliation, nature and daily reach (June 2019)

NEWSPAPER	POLITICAL ORIENTATION	DAILY REACH	NATURE
The Sun	Conservative (strong)	2,818,000	Tabloid
Daily Mail	Conservative (strong)	2,675,000	Tabloid
Metro	Unconfirmed	2,438,000	Tabloid
Evening Standard	Conservative	1,181,000	Tabloid
The Times	Conservative (weak)	1,113,000	Quality
Daily Mirror	Labour (strong)	1,032,000	Tabloid
Daily Telegraph	Conservative (moderate)	864,000	Quality
The Guardian	Liberal democrat (moderate)	653,000	Quality
Daily Express	Conservative (very strong)	605,000	Tabloid
Daily Star	Right-centre	507,000	Tabloid

Source: PAMCo (2019); Wring & Deacon (2010)

Considering that Table 1 shows the top 10 newspapers in the UK according to daily reach, this research disregarded both newspapers that are freesheet, i.e. free of charge, namely *Metro* and *Evening Standard*. In addition, as this list has only three quality newspapers, this research selected also three tabloid newspapers, in order to have a final sample of six newspapers (see Table 2).

Table 2: Selected UK newspapers by political affiliation, nature and daily reach (June 2019)

NEWSPAPER	POLITICAL ORIENTATION	DAILY REACH	NATURE
The Sun	Conservative (strong)	2,818,000	Tabloid
Daily Mail	Conservative (strong)	2,675,000	Tabloid
The Times	Conservative (weak)	1,113,000	Quality
Daily Mirror	Labour (strong)	1,032,000	Tabloid
Daily Telegraph	Conservative (moderate)	864,000	Quality
The Guardian	Liberal democrat (moderate)	653,000	Quality

Source: PAMCo (2019); Wring & Deacon (2010)

This composition assures that this research includes the same number of tabloid and quality newspapers: three of each. In addition, it comprises diverse political views, although there is a general predominance of Conservative newspapers, as they are the most read in the country. In fact, this selection comprises titles that are considered Conservative (strong, moderate and weak), Labour (strong) and Liberal Democrat (moderate) – with at least one non-Conservative newspaper among the tabloids (*Daily Mirror*) and another one among quality newspapers (*The Guardian*). Regarding daily reach, this sample includes newspapers that vary from 2,675,000 (*Daily Mail*) to 653,000 (*The Guardian*). It is worth mentioning here that although this research considers the print versions of these six newspapers, their readership is considerably increased when including online readers that have access to the same articles. In the case of *The Guardian*, for instance, the daily reach is amplified through more than 15 million readers when considering people that access their news via mobile phones, tablets, personal computers and other platforms (Newsworks, 2019). The same is seen for the other titles, and this helps to unveil the significance of these newspapers to the circulation of information.

3.5 Data Collection

Considering that this research aims to unveil the British press's representation of Deep Web technologies, using content analysis and critical discourse analysis, newspaper articles are the unit of analysis. Prior to the data collection, however, this research requires two primary steps: one in regards to the proper content that needs to be collected, and another one related to the time frame. On the first point, a preliminary survey helped uncover the terms usually related to Deep Web technologies among the selected newspapers and led to finding the following keywords – organised in alphabetical order and not in relevance, in Table 3 – to be included in the data collection. These 27 keywords were each found at least once making reference to the Deep Web technologies.

Table 3: Keywords selected for the data collection

1	"dark internet"
2	"dark net"
3	"dark side of the internet"
4	"dark side of the web"
5	"dark web"
6	"darknet"
7	"darkweb"
8	"deep internet"
9	"deep web"
10	"hidden internet"
11	"hidden web"
12	"internet dark side"
13	"invisible internet"
14	"invisible web"
15	"non-indexable internet"
16	"non-indexable web"
17	"silk road"
18	"silkroad"

19	"tor browser"
20	"tor network"
21	"tor system"
22	"undernet"
23	"underweb"
24	"underworld of the internet"
25	"underworld of the web"
26	"web dark side"
27	"web underworld"

Regarding the time frame for data collection, this research includes all articles mentioning one or more of these keywords following the first appearance of articles up to 31st December 2017 – this was selected as the limit, because the following years were used to conduct the content analysis and the critical discourse analysis, as well as organise findings and discussions. Finally, data collection was ensured through the Lexis-Nexis Database, accessible through the Loughborough University Library website with a personal login. This software allows for gathering a large amount of data when analysing newspapers, since it offers content from thousands of editions issued by hundreds of titles, with searches crossing customised dates and keywords. Using Lexis-Nexis, however, can create methodological implications concerning information validity and reliability, as argued by Deacon (2007), as the researcher relies on the results provided by the online database instead of looking for the content straight from the source. In fact, Lexis-Nexis changed the way in which content analysis is done, by providing larger samples and separating digital versions from print media, among other functionalities (Deacon, 2007). As noted by Deacon (2007, p. 29), this is a compelling resource if adopting precautions such as 'checking for "false positives" and duplicated items, scanning the titles and periods sampled for any high-level omissions in data, and checking items for inconsistent unitization.'

For this study, data collection through Lexis-Nexis involved one newspaper at a time and two search phases. In addition, the starting date selected was 1st January 1989, symbolising the year in which the Web was invented; in practice, though, the first articles about the Deep Web technologies date from the 2000s, as shown in the analysis which follows. Considering this point,

the first phase includes 25 terms used interchangeably to define the Deep Web and selecting the entire period of this research, from 1989 to 2017 (see Table 4).

Table 4: Parameters of the search on Lexis-Nexis (phase 1)

TIME FRAME	From 01/01/1989 to 31/12/2017
KEYWORDS	"dark internet" or "dark net" or "dark side of the internet" or "dark side of the web" or "dark web" or "darknet" or "darkweb" or "deep internet" or "deep web" or "hidden internet" or "hidden web" or "internet dark side" or "invisible internet" or "invisible web" or "non-indexable internet" or "non-indexable web" or "tor browser" or "tor network" or "tor system" or "undernet" or "underweb" or "underworld of the internet" or "underworld of the web" or "web dark side" or "web underworld"

Moreover, the second phase focused on news about the crypto market Silk Road. Considered the most famous market on the Tor Network, Silk Road was launched in February 2011 and ran on Onion Services for over two years, until its closure by the FBI in October 2013 (Aldridge & Décary-Hétu, 2014). Thereafter, other sites were created similar this one, to replace it, even claiming names such as Silk Road 2.0. For this reason, the search for the two remaining keywords – "silk road" and "silkroad" – applied only to the period between 1st January 2011 and 31st December 2017 (see Table 5).

Table 5: Parameters of the search on Lexis-Nexis (phase 2)

TIME FRAME	From 01/01/2011 to 31/12/2017
KEYWORDS	"silkroad" or "silk road"

This division into two phases proved itself helpful in reducing the number of false positives, since Silk Road is also the name of the complex terrestrial and maritime routes crossing Asia and Europe and used for trade in ancient times. In fact, significant numbers of false positives among

those collected by Lexis-Nexis are related to touristic incursions to the Silk Road or, more recently, to the construction of the Eurasian Land Bridge, a transcontinental rail transport route the aim of which is to connect Pacific seaports in Russia and China with seaports in Europe. It is also referred to as the "New Silk Road." In addition, considering Lexis-Nexis's functionalities, another point about data collection is that the researcher can choose whether or not to include duplicates, website articles and other options (see Figure 9). In the case of this research, the data include only news items that were published in the print version of the newspapers, as a strategy to narrow down the amount of data and be sure that the final version could be analysed.

Figure 9: Nexis options during the search
Source: https://www.lexisnexis.com/
Retrieved by the author in October 2019

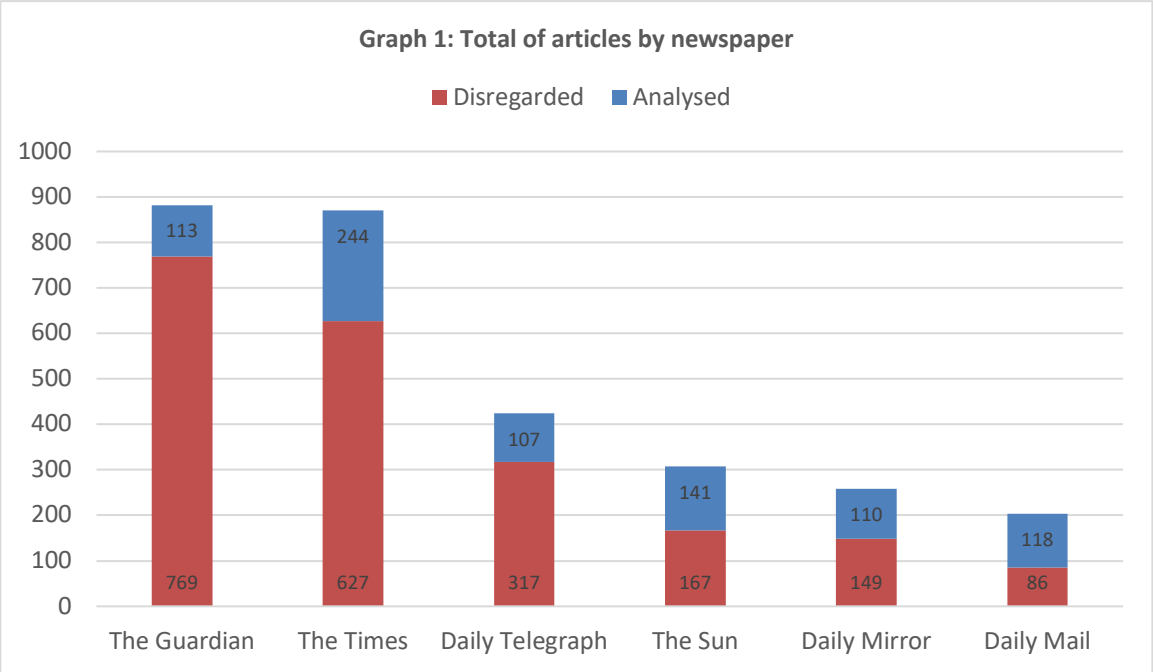
After these two phases, the data collection sample reached 2,948 articles, which were all downloaded for further investigation and saved onto the university's servers (see Table 6).

Table 6: Data collection on Nexis by newspaper

NEWSPAPER	NUMBER OF ARTICLES		
	PHASE 1	PHASE 2	TOTAL
Daily Mail	163	41	204
Daily Mirror	205	54	259
Daily Telegraph	190	234	424
The Guardian	569	313	882
The Times	544	327	871

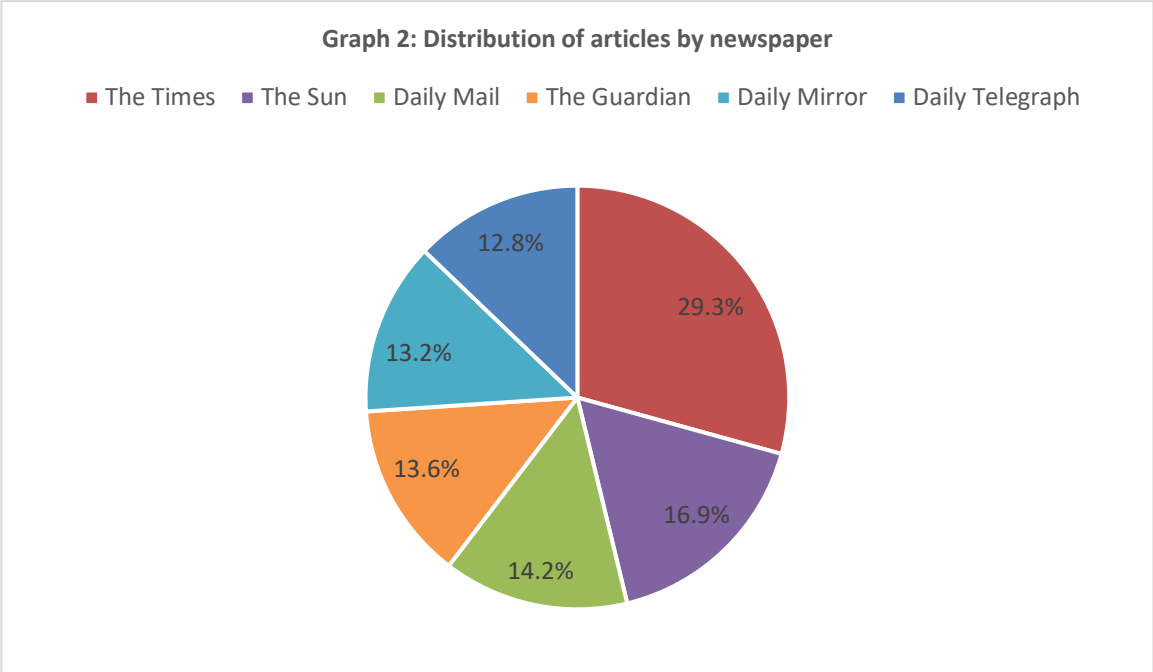
The Sun	261	47	308
Total	1,932	1,016	2,948

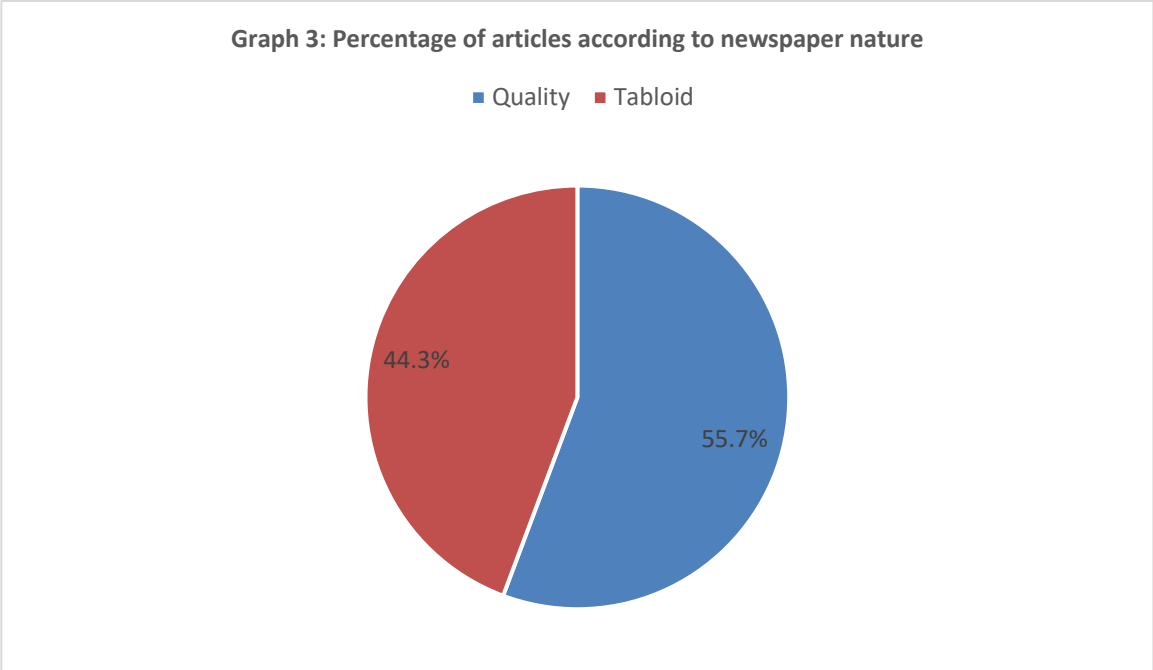
After collecting the newspaper articles, the following step was to disregard duplicates and false positives. In the case of duplicates, the most common type was the same article being published in multiple editions of the same newspaper – not just the first, but also second, third and, in some cases, fourth editions. Considering that the latest edition is theoretically the most up to date version, this research includes in the analysis just those articles published in the latest edition. Also, in some cases, the same applied to editions circulating in distinct territories, i.e. national and Scottish editions. In this event, this research prioritised the national edition, considering that it had a greater reach. In consideration of false positives, these were ignored when they were not related to the Deep Web technologies, previously defined as content not indexed by regular search engines and/or accessible through Tor. These included articles about Silk Road, but related to the real route connecting Asia and Europe, not the crypto market; articles mentioning "the dark side of the internet" in a context of online bullying on the Surface Web; articles referring to a "hidden web of lies" or "dark web of criminals," among other combinations of words, which are not specifically related to these technologies. Therefore, by applying these filters, data for coding were considerably reduced to 833 articles from the initial 2,948 articles, thereby disregarding 2,115 duplicates and false positives (see Graph 1).



It is worth mentioning here that a challenge imposed on this research regarded content published by *The Guardian*, and so data collection demanded an additional effort, since this newspaper does not specify on Lexis-Nexis, since September 2014, if the article was published in the print version of the newspaper or just on the website. After consulting the Nexis Support Team as well as the information department at *The Guardian*, it was necessary to use the website ClipSearch,[27] through NLA Media Access, to review news items published in the print version. In summary, this software provides open access to news titles, dates of publication and page numbers for *The Guardian* print version, which is enough information to assure that the article was published in the print version. This task was time-consuming, but effective. Regarding the final number of articles, Graphs 2 and 3 provide some initial insights into how the sample is composed.

[27] Available on http://www.clipsearch.co.uk/ Access: October 2019.





As perceived from the above graphs, there is an overall balanced number of articles among quality (55.7%) and tabloid (44.3%) newspapers, with a higher number published by the first type, due potentially to the fact that *The Times* makes up 29.3% of the publications. The other

newspapers present publication percentages varying between 16.9% and 12.8%. Considering these data, the next sections focus on the methods used in the analysis.

3.6 Content Analysis

Examining the history of newspaper analysis, Krippendorf (2013) argues that the increase in information mass production at the beginning of the 20th century demanded an objective consideration of this phenomenon as well as its potential consequences to society; in this sense, quantitative analysis of newspapers was developed to help pursue scientific rigour, initially concerned with the space dedicated to distinct topics. Content analysis focusing on the message was established only in the 1940s and was used by sociologists studying media impacts on public opinion in terms of political, social and economic matters, but nowadays it is spread across disciplines, such as the study of documents, books and social media (Krippendorf, 2013). As noted by Krippendorf (2013), content analysis is an exploratory method used to explain how messages are communicated and meaning constructed, which is why it is a suitable social research method for understanding representations through media messages.

Riffe, Lacy & Fico (2005, p. 3) define content analysis as 'the systematic assignment of communication content to categories according to rules, and the analysis of relationships involving those categories using statistical methods.' This quantitative approach is considered relevant in the context of mass communication research, not only to identify ideas sent through media outlets, but also due to the potential consequences of being exposed to these messages, including a changing in attitude and thinking in society (Riffe et al., 2005). Although it is not a new method, content analysis constantly benefits from technological developments, since there is a continuous improvement in software alternatives to assist researchers conducting their studies with larger samples to save time (Neuendorf, 2002). These resources help content analysis remain systematic, in order to retain scientific validity and objectivity. In practice, this method demands a structured approach which includes, according to Neuendorf (2002), defining the sample, time frame and unit of analysis, collecting data, developing a codebook, coding, testing coding reliability and analysing results. As most of these points have already been addressed in this chapter, this section explains the construction of the codebook.

Constructing the Codebook

A crucial part of the systematic protocol required to proceed with content analysis, the codebook can be defined as a manual that aggregates all the variables being measured on analysed content, as well as instructions to avoid ambiguities amongst coders (Neuendorf, 2002). Therefore, constructing an original codebook is a process that requires time, revisions and confirmation through reliability tests; in fact, in the case of this research, constructing the codebook proved itself a challenging and time-consuming step. The final version of the codebook (see Appendix) is composed of two main parts: the first presents the case identification variables, and the other introduces the content variables. Five variables are used to identify each article: (V01) an ID number, created to provide a unique code for each article; (V02) date of publication; (V03) newspaper; (V04) type of article, including news article, editorial, reader's comment/opinion, review of books or others, interview and fiction, and (V05) length of the text (number of words).

In relation to content variables, 18 points are investigated in this research. To start, it identifies (V06) if the Deep Web technologies are mentioned in the headline of the article and (V07) which term is used, from a list of 20 terms interchangeably used by the six analysed newspapers. For the headline, the codebook checks if (V08) there is mention of anything from a list of 15 distinct activities, such as drugs, financial fraud, hacking, paedophilia, pornography and others. This variable was included to measure to what extent articles that mention the Deep Web are related to criminal and antisocial behaviours exemplified for these activities.

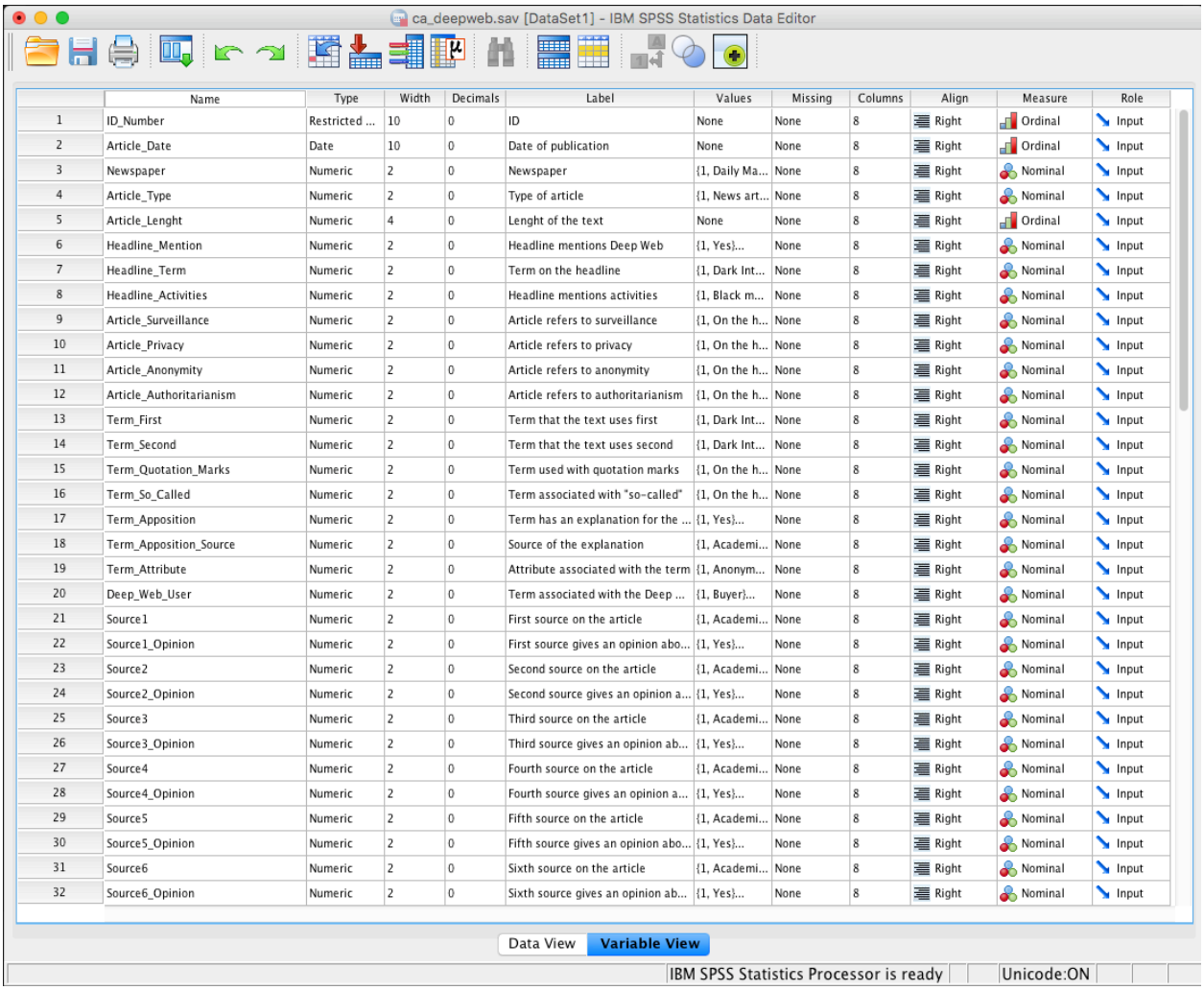
Considering that this study connects the uses of the Deep Web to the contemporary culture of surveillance, this codebook also focuses on understanding how the British press associates the use of these technologies with privacy issues. Therefore, this codebook measures (V09) if the article mentions surveillance practices – including a list of keywords such as "tracking," "monitoring" and others – and what relevance is given to the topic (the headline, the text, both the headline and the text or none of them). The same applies for (V10) privacy issues, including keywords such as "personal data," "secrecy" and others; (V11) "anonymity," also "invisibility" and "pseudonym," among others, and (V12) "authoritarianism," as well as "fascism," "tyranny" and others.

In terms of the way the Deep Web is presented in the text, this codebook also reviews: (V13) the first term that is used in the text to refer to these technologies; (V14) the second term, if it is the case that two terms are mentioned; (V15) if the term is mentioned between quotation marks, or not; (V16) if it is associated with the expression "so-called," or not; (V17) if the article offers an apposition (explanation or definition) connected to the term and, if so, (V18) the source of this apposition, from academics to law enforcement; (V19) what attribute is associated with or used to describe the term and (V20) what term is associated with the people that use Deep Web technologies. Finally, the last variables in the codebook are dedicated to sources that are quoted or paraphrased in the article. As such, the aim is (V21) to identify the source from a number of possibilities, such as academic, government, victim and others, and (V22) to recognise if the source is actively talking about the Deep Web technologies or not. The same variables are applied to every source mentioned in the article, adding V23 and V24, V25 and V26, V27 and V28 and so on. It is worth mentioning here that the highest number of sources among the researched articles was 12.

The Challenges of Coding

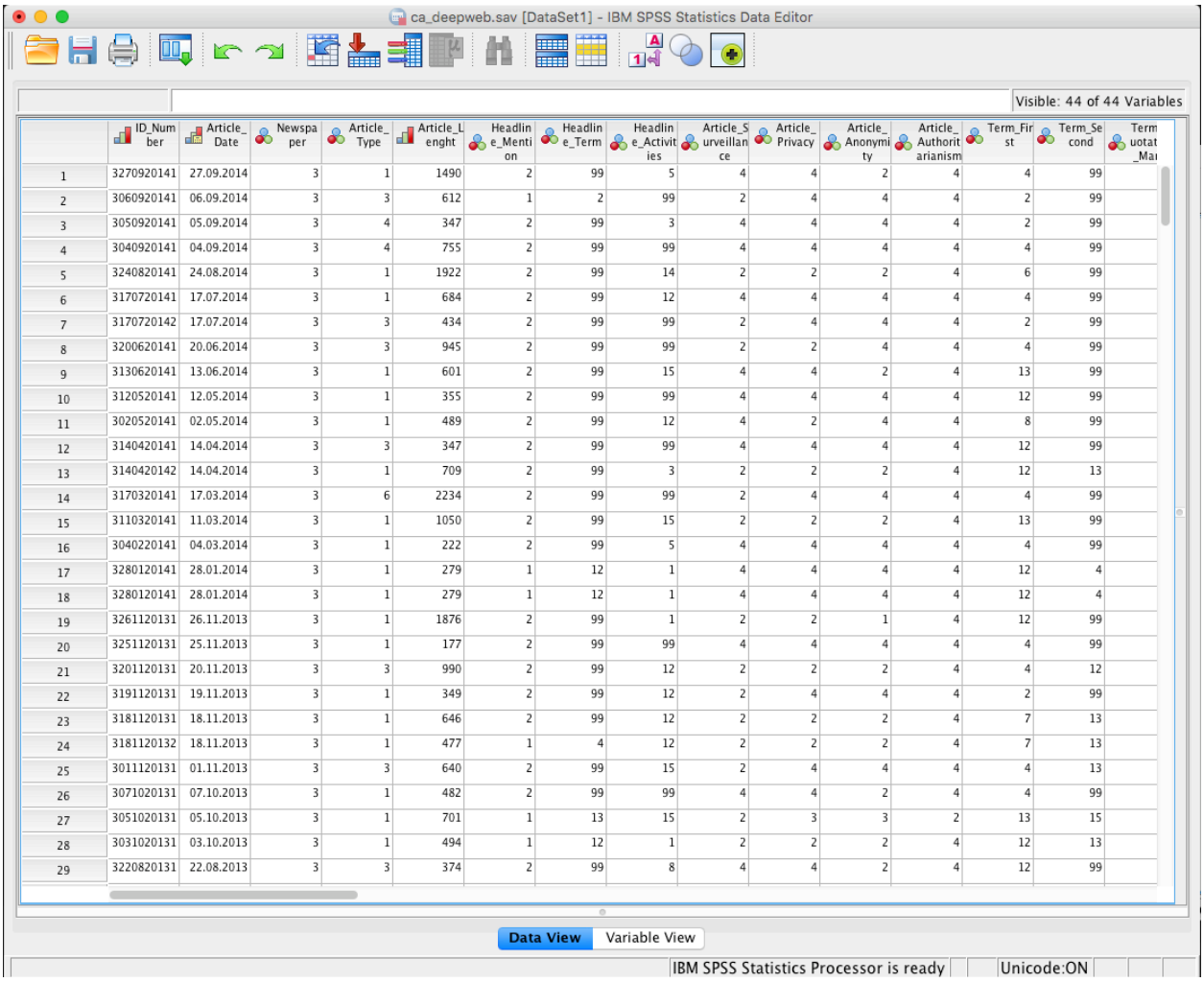
As content analysis requires time and training, a relevant part of this method is related to coding preparation, also called practice or pilot, which is necessary to assure the reliability of the codebook (Neuendorf, 2002). In summary, the codebook demands a series of assessments, followed by reviews and adjustments, until it is considered ready to be used, and in this case, the researcher pursued a codebook without ambiguities on variables, values and instructions. The process of manual coding, in practice, demands a systematic approach to maximising time and keeping the same standards from beginning to end, thereby protecting data validity (Neuendorf, 2002). This process can be done in multiple ways, and in the case of this study, the coder opted to use hard copies of newspaper articles, in order to highlight relevant data on the pages and at the same time not rely on technology for the text analysis. The coding, however, was done through IBM SPSS Statistics 25, software offered by Loughborough University. Using this software requires two main phases: first, inserting the variables with the related code value and label (see

Figure 10), and then coding, which means analysing each newspaper article through all the variables in the codebook, resulting in one line of code (see Figure 11).



	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	ID_Number	Restricted ...	10	0	ID	None	None	8	Right	Ordinal	Input
2	Article_Date	Date	10	0	Date of publication	None	None	8	Right	Ordinal	Input
3	Newspaper	Numeric	2	0	Newspaper	{1, Daily Ma...	None	8	Right	Nominal	Input
4	Article_Type	Numeric	2	0	Type of article	{1, News art...	None	8	Right	Nominal	Input
5	Article_Lenght	Numeric	4	0	Lenght of the text	None	None	8	Right	Ordinal	Input
6	Headline_Mention	Numeric	2	0	Headline mentions Deep Web	{1, Yes}...	None	8	Right	Nominal	Input
7	Headline_Term	Numeric	2	0	Term on the headline	{1, Dark Int...	None	8	Right	Nominal	Input
8	Headline_Activities	Numeric	2	0	Headline mentions activities	{1, Black m...	None	8	Right	Nominal	Input
9	Article_Surveillance	Numeric	2	0	Article refers to surveillance	{1, On the h...	None	8	Right	Nominal	Input
10	Article_Privacy	Numeric	2	0	Article refers to privacy	{1, On the h...	None	8	Right	Nominal	Input
11	Article_Anonymity	Numeric	2	0	Article refers to anonymity	{1, On the h...	None	8	Right	Nominal	Input
12	Article_Authoritarianism	Numeric	2	0	Article refers to authoritarianism	{1, On the h...	None	8	Right	Nominal	Input
13	Term_First	Numeric	2	0	Term that the text uses first	{1, Dark Int...	None	8	Right	Nominal	Input
14	Term_Second	Numeric	2	0	Term that the text uses second	{1, Dark Int...	None	8	Right	Nominal	Input
15	Term_Quotation_Marks	Numeric	2	0	Term used with quotation marks	{1, On the h...	None	8	Right	Nominal	Input
16	Term_So_Called	Numeric	2	0	Term associated with "so-called"	{1, On the h...	None	8	Right	Nominal	Input
17	Term_Apposition	Numeric	2	0	Term has an explanation for the ...	{1, Yes}...	None	8	Right	Nominal	Input
18	Term_Apposition_Source	Numeric	2	0	Source of the explanation	{1, Academi...	None	8	Right	Nominal	Input
19	Term_Attribute	Numeric	2	0	Attribute associated with the term	{1, Anonym...	None	8	Right	Nominal	Input
20	Deep_Web_User	Numeric	2	0	Term associated with the Deep ...	{1, Buyer}...	None	8	Right	Nominal	Input
21	Source1	Numeric	2	0	First source on the article	{1, Academi...	None	8	Right	Nominal	Input
22	Source1_Opinion	Numeric	2	0	First source gives an opinion abo...	{1, Yes}...	None	8	Right	Nominal	Input
23	Source2	Numeric	2	0	Second source on the article	{1, Academi...	None	8	Right	Nominal	Input
24	Source2_Opinion	Numeric	2	0	Second source gives an opinion a...	{1, Yes}...	None	8	Right	Nominal	Input
25	Source3	Numeric	2	0	Third source on the article	{1, Academi...	None	8	Right	Nominal	Input
26	Source3_Opinion	Numeric	2	0	Third source gives an opinion ab...	{1, Yes}...	None	8	Right	Nominal	Input
27	Source4	Numeric	2	0	Fourth source on the article	{1, Academi...	None	8	Right	Nominal	Input
28	Source4_Opinion	Numeric	2	0	Fourth source gives an opinion a...	{1, Yes}...	None	8	Right	Nominal	Input
29	Source5	Numeric	2	0	Fifth source on the article	{1, Academi...	None	8	Right	Nominal	Input
30	Source5_Opinion	Numeric	2	0	Fifth source gives an opinion abo...	{1, Yes}...	None	8	Right	Nominal	Input
31	Source6	Numeric	2	0	Sixth source on the article	{1, Academi...	None	8	Right	Nominal	Input
32	Source6_Opinion	Numeric	2	0	Sixth source gives an opinion ab...	{1, Yes}...	None	8	Right	Nominal	Input

Figure 10: IBM SPSS Statistics screenshot (variable view)
Retrieved by the author in October 2019



	ID_Number	Article_Date	Newspaper	Article_Type	Article_Lenght	Headline_Mention	Headline_Term	Headline_Activities	Article_Surveillance	Article_Privacy	Article_Anonymity	Article_Authoritarianism	Term_First	Term_Second	Term_Quotation_Mar
1	3270920141	27.09.2014	3	1	1490	2	99	5	4	4	2	4	4	99	
2	3060920141	06.09.2014	3	3	612	1	2	99	2	4	4	4	2	99	
3	3050920141	05.09.2014	3	4	347	2	99	3	4	4	4	4	2	99	
4	3040920141	04.09.2014	3	4	755	2	99	99	4	4	4	4	4	99	
5	3240820141	24.08.2014	3	1	1922	2	99	14	2	2	2	4	6	99	
6	3170720141	17.07.2014	3	1	684	2	99	12	4	4	4	4	4	99	
7	3170720142	17.07.2014	3	3	434	2	99	99	2	4	4	4	2	99	
8	3200620141	20.06.2014	3	3	945	2	99	99	2	2	4	4	4	99	
9	3130620141	13.06.2014	3	1	601	2	99	15	4	4	2	4	13	99	
10	3120520141	12.05.2014	3	1	355	2	99	99	4	4	4	4	12	99	
11	3020520141	02.05.2014	3	1	489	2	99	12	4	2	4	4	8	99	
12	3140420141	14.04.2014	3	3	347	2	99	99	4	4	4	4	12	99	
13	3140420142	14.04.2014	3	1	709	2	99	3	2	2	2	4	12	13	
14	3170320141	17.03.2014	3	6	2234	2	99	99	2	4	4	4	4	99	
15	3110320141	11.03.2014	3	1	1050	2	99	15	2	2	2	4	13	99	
16	3040220141	04.03.2014	3	1	222	2	99	5	4	4	4	4	4	99	
17	3280120141	28.01.2014	3	1	279	1	12	1	4	4	4	4	12	4	
18	3280120141	28.01.2014	3	1	279	1	12	1	4	4	4	4	12	4	
19	3261120131	26.11.2013	3	1	1876	2	99	1	2	2	1	4	12	99	
20	3251120131	25.11.2013	3	1	177	2	99	99	4	4	4	4	4	99	
21	3201120131	20.11.2013	3	3	990	2	99	12	2	2	2	4	4	12	
22	3191120131	19.11.2013	3	1	349	2	99	12	2	4	4	4	2	99	
23	3181120131	18.11.2013	3	1	646	2	99	12	2	2	2	4	7	13	
24	3181120132	18.11.2013	3	1	477	1	4	12	2	2	2	4	7	13	
25	3011120131	01.11.2013	3	3	640	2	99	15	2	4	4	4	4	13	
26	3071020131	07.10.2013	3	1	482	2	99	99	4	4	2	4	4	99	
27	3051020131	05.10.2013	3	1	701	1	13	15	2	3	3	2	13	15	
28	3031020131	03.10.2013	3	1	494	1	12	1	2	2	2	4	12	13	
29	3220820131	22.08.2013	3	3	374	2	99	8	4	4	2	4	12	99	

Figure 11: IBM SPSS Statistics Data Editor screenshot (data view)
Retrieved by the author in October 2019

Relevant to this process, the first intercoder reliability test was done on October 2017, when discussions about the codebook were exhausted and the document was considered ready for assessment. During this test, two independent coders applied the variables to 10 randomly chosen articles. Using the website Recal2[28] to compare results and calculate coefficients, the percentage of agreement was 89% (see details in Table 7). Also, the coefficients Krippendorff's Alpha, Scott's Pi and Cohen's Kappa were .0876. Although this number is considered excellent,

[28] Available on http://dfreelon.org/utils/recalfront/recal2/ Access: October 2017.

with higher reliability (Neuendorf, 2002), the codebook was adjusted according to the coders' feedback, reducing even more the chances of future coding disagreements.

Table 7: Intercoder reliability test results

Coders	2
Cases	200
Number of agreements	178
Number of disagreements	22
Percent of agreement	89%
Krippendorff's Alpha	.876
Scott's Pi	.876

Finally, the process of coding was time-consuming, as initially expected, because only one researcher was responsible for the analysis of 833 newspaper articles according to a minimum of 22 variables each; in addition, in the cases of 12 distinct sources in the article, this number rose to 44 variables. Moreover, content analysis requires very thorough work, which in this case was conducted completely manually. This means reading and coding one by one each of the 833 articles, with an average of 579 words each, a total of 482,448 words – the equivalent of six doctoral theses.

3.7 Critical Discourse Analysis

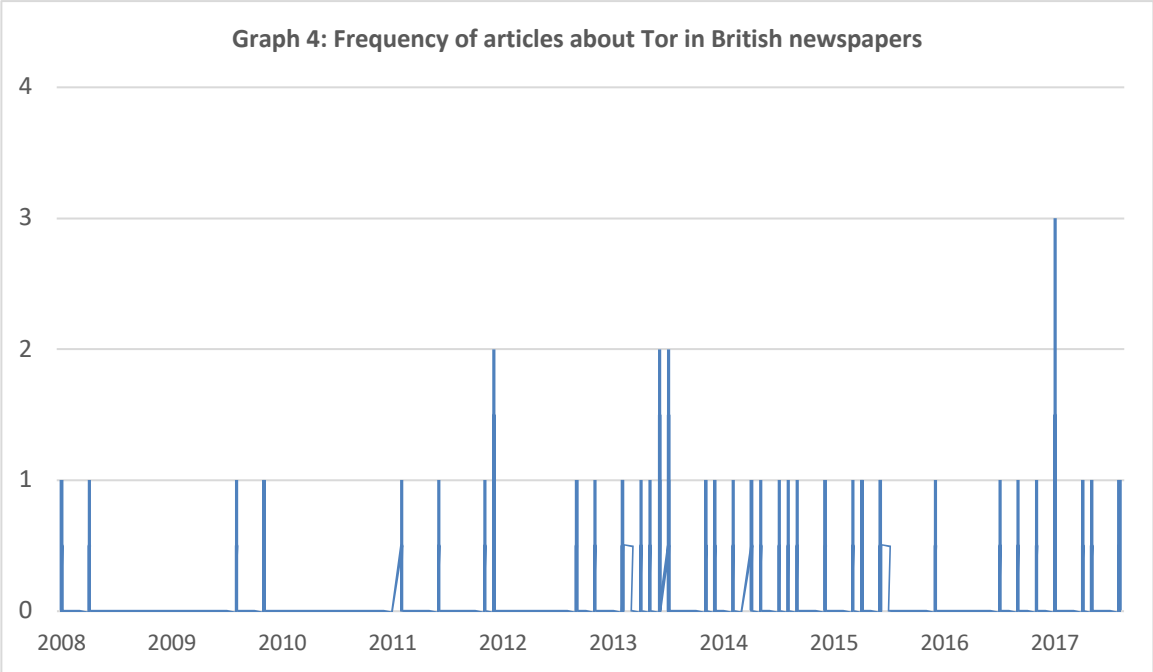
As noted by van Dijk (1993, p. 250), critical discourse analysis in principle is related to challenging social power – related to privileges, such as access to wealth and education – and dominance – seen as a form of power – establishing a critique of the 'elites and their discursive strategies for the maintenance of inequality.' Arguing about discourse and communication as a resource through which social power and dominance are based, van Dijk (1993, p. 256) states that 'an analysis of the various modes of discourse access reveals a rather surprising parallelism

between social power and discourse access: the more discourse genres, contexts, participants, audience, scope and text characteristics they (may) actively control or influence, the more powerful social groups, institutions or elites are.' Furthermore, van Dijk (1993, p. 258) asserts that the core of critical discourse analysis is related to 'a detailed description, explanation and critique of the ways dominant discourses (indirectly) influence such socially shared knowledge, attitudes and ideologies, namely through their role in the manufacture of concrete models,' and with this being able to understand how social representations are constructed.

Reflecting on the discourse of news media, Chimombo & Roseberry (1998, p. 311) argue that media outlets provide rich data for researchers about the culture in which they are inserted, since 'it is the job of the news media to interpret cultural matters for local understanding.' Nonetheless, analysing newspapers also presents multiples aspects that shall be considered, such as uncertainty about the author, since writing a news article is not a lonely process; the relationship between the producer (journalist) and interpreters (audience); the topic in itself and why facts have distinct significance; the setting chosen when writing about a topic; the purpose of the article and also the intent when the structure is built, in terms of information hierarchy (Chimombo & Roseberry, 1998). According to Paltridge (2006, p. 179), critical discourse analysis 'explores the connections between the use of language and the social and political contexts in which it occurs,' thereby combining textual analysis with the interpretation of what a discourse represents at that specific moment in time. These and other considerations are taken into account in Chapters 6 (*the Tor Network, Liberation Technology and Hopes*) and 7 (*the Tor Network, Technological Ambivalence and Polarisation*).

In the case of this research, critical discourse analysis complements the content analysis previously conducted, consequently providing deeper and richer insights about how Deep Web technologies are portrayed by the British press. As a way of narrowing down the sample and making the critical discourse analysis feasible, however, it was necessary to choose a fragment of the articles instead of analysing 833 publications. As a result, this critical discourse analysis is applied only to articles mentioning the Tor Network, which means 58 articles in total. This number represents the total numbers of articles about Tor in the six British newspapers, and no article mentioning Tor was disregarded. This sample was therefore a side-product of the coding,

considering that variables V07, V13 and V14 refer specifically to terms used in the article and/or headline, including the Tor Network as well as variations (Onion Router, Tor, Tor Browser). Although Tor was founded in 2002, coverage started only in 2008, as Graph 4 illustrates, showing the frequency of publications over time.



In terms of the sample used in the critical discourse analysis, from the final number of 58 articles mentioning Tor, 50 were published by quality newspapers and only eight by tabloid: 23 articles by *The Guardian*, 22 by *The Times*, five by *The Daily Telegraph*, four by *The Sun*, three by *Daily Mirror* and only one by *Daily Mail*. This shows the scant interest of British tabloids on the topic during the researched time frame, which is addressed in the analysis and discussion.

3.8 Ethical Considerations

Taking into account that this research analyses newspaper articles considered public domain content and not private information, this work was not obliged to obtain formal consent from

the Ethics Approvals (Human Participants) Sub-Committee of Loughborough University[29], and therefore there were no restrictions involved in collecting and analysing these data. It is worth noting, however, that this work does not ignore the negative uses of Deep Web technologies, which in itself leads to the emergence of an ethical discussion. The Tor Network, for instance, provides online anonymity which, on the one hand, protects vulnerable groups, ensures safe communications and helps those fighting for human rights, while on the other hand it creates a safe haven for criminal activity. As such, this research understands that Tor's existence and public availability do not exist in harmony, and so the discussions on this topic introduced in the literature review are revisited in the next four analytical chapters.

[29] More information at http://www.lboro.ac.uk/committees/ethics-approvals-human-participants/ Access: October 2019.

4 The Struggle in Defining Meaning and Concept: A Deep or a Dark Web?

This thesis presents an empirical study focused on British press representations of Deep Web systems, uses and users. Consequently, it proposes an introductory examination of the concepts that are used and the definitions provided related to these technologies. This chapter therefore discusses the choices of terms, associations and explanations offered by six British newspapers to unveil how meaning is constructed in the context of the Deep Web. As noted by Gitelman & Pingree (2003, xii), when a new medium emerges, it often goes through a phase of 'identity crisis,' which is overcame by adapting the technology and its uses to the public understanding. Traditional media play a relevant role in this process, not only by presenting new elements to the public and creating culture, meaning and knowledge, but also by normalising views and ideologies (Fürsich, 2010; Kidd, 2016; Orgad, 2012). As previously addressed, the Deep Web allows various uses, including positive ones such as enabling online anonymity (Hoang & Pishva, 2014), archiving content on databases (Kendrick, 2007; Pedley, 2002; Su, 2008; Sui et al., 2015; Theng et al., 2016), limiting surveillance (Floridi, 2014), protecting communications (Baek et al., 2016; Bellare & Rogaway, 2005; van Baalen, 2018), assuring freedom of speech (Jardine, 2018a; Sharon & John, 2018; Wu & Atkin, 2018), escaping digital tracking (Dingledine et al., 2004) and more. This chapter argues, however, that this technology is largely presented by the British press in only one dimension: a secretive tool used for negative (or at least questionable) purposes.

4.1 The Deep Web and the British Press: an Introduction

The general discourse about technology in the press and other media is often shaped through hopes and fears related to societal, economic and political aspects (Natale & Ballatore, 2014; Sturken et al., 2004). The Web, for instance, demonstrates how representations include hope surrounding positive uses, and the fear of negative ones (Malbreil, 2007; Mosco, 2004). Considering that technology encourages myths (Mosco, 2004) and interpretations that reflect on social and cultural construction (Natale & Balbi, 2014), the imaginary is over-stimulated in the case of the Web: it has changed human relations challenging the ideas of space and time

(Malbreil, 2007) and encouraged media changes and evolution (Natale & Balbi, 2014). Overall, in the past, the Web was heralded in predominantly positive tones, due to an idealistic view of the Internet (Flichy, 2007; Mosco, 2006; Streeter, 2011). Negative uses, however, are evident: spam (Brunton, 2013), the destructive impact of social media (Van Dijck, 2013), private corporations jeopardising personal privacy (Striphas, 2015), state abuse (Greenwald, 2014), fake news (Vargo et al., 2018) and cyberattacks (Landau, 2017) re just a few examples in this regard. Although, nowadays, the discourse about the Web generally balances positive and negative uses, the British press do not offer the same treatment and courtesy to the Deep Web. In fact, these systems are often portrayed as the source of all evil in the digital world, as stated by an article[30] published by *Daily Mirror*[31] in 2017, presenting a scenario not only in which the Dark Web is seen as threatening, but also where other Internet users are portrayed as harmless and innocent in opposition:

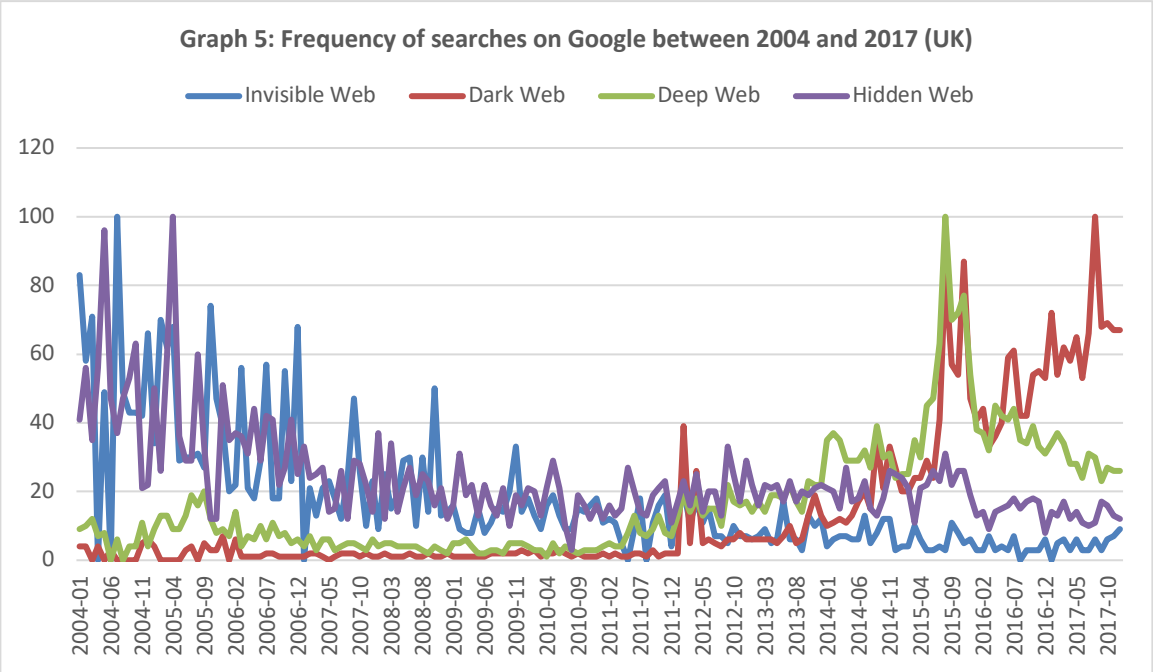
> The Dark Web is unknown to the millions of people who innocently use the net every day […] It is time the forces of the law and order began concentrating their resources on this hidden menace. Only then will the scourge of the dark web be dragged into the light.

Even the choice of using one or another term in the daily coverage of newspapers, for instance "Dark Web" instead of "Deep Web," contributes to this imaginary. Indeed, representation is connected to concepts, i.e. names for things that need to be explained or codified to make sense in the world (Loocke, 1999) and signify the general knowledge about experiences in the world (Bolton, 1997), and which can evolve and change over time (Koselleck, 2002). Moreover, conceptual history is related to comprehending lived experiences and theorising about historical change through reworked concepts (Müller, 2014) intrinsically connected to interpretations (Kelley, 1996) with an ideological dimension (Melton, 1996). In academia, the first concept widely employed about these technologies was the "Invisible Web"

[30] For the purpose of better readability, this thesis includes references to the newspaper articles that are analysed and mentioned as footnotes throughout the chapters.
[31] Related article: "No safety net for the dark web," Daily Mirror, 6th August 2017, page 14.

(Ellsworth & Ellsworth, 1994), defining the entire body of Web content outside traditional platforms. Nevertheless, this term is still used (Devine & Egger-Sider, 2014), although it is criticised for being overly generic (Shestakov, 2008) or inaccurate (Bergman, 2001). Since the early 2000s, the "Deep Web" concept (Bergman, 2001) has opposed the idea of an "Invisible Web," since this content is hidden but still visible. In addition, terms such as "Hidden Web" and "Deep Web" are considered interchangeable, in that using one or the other depends on preference (Shestakov, 2008). A similar dynamic is observed on Google Trends, a service provided by Google that allows people to collect data about searches regarding terms, locations and dates. Examining the searches on the topic since 2004[32] in the United Kingdom (Graph 5), there was a growing interest in the "Deep Web" [33] until August 2015, when searches fell consistently. Although with consistent occurrences over time, the term "Invisible Web"[34] peaked in March 2004 and became less relevant after November 2006. "Hidden Web"[35] followed the same trend, with both alternating positions until 2012.

[32] As Google was founded in 2004, there are no previous data on the topic. This work includes the time frame between January 2004 and December 2017.
[33] Available on https://trends.google.com/trends/explore?date=all&geo=GB&q=%22deep%20web%22 Access: November 2018.
[34] Available on https://trends.google.com/trends/explore?date=all&geo=GB&q=%22invisible%20web%22 Access: November 2018.
[35] Available on https://trends.google.com/trends/explore?date=all&geo=GB&q=%22hidden%20web%22 Access: November 2018.



The term "Dark Web"[36], however, peaked first in searches in February 2012, and since then it has consistently grown on a monthly basis, becoming the most searched term from the beginning of 2016. This shows a pattern within social imaginaries that helps create meaning and sense around technological innovations (Mansell, 2012): from the Deep to the Dark Web. Using one or the other concept is part of a chain that starts in the imaginary in relation to technology, makes different interpretations and uses and reflects in the technology's social and cultural construction (Natale & Balbi, 2014). While terms such as "Deep Web" and "Invisible Web" have dominated academic discussion, the increasing attention of popular media towards this phenomenon has tended towards a different term: "Dark Web." As a matter of fact, 2015 was an important year for this concept, since it was shortlisted for "Word of the Year" by the Oxford Dictionaries, although the emoji known as "face with tears of joy"[37] gained the title in the end. The definition given by the dictionary is thus: 'Dark Web, noun: The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to

[36] Available on https://trends.google.com/trends/explore?date=all&geo=GB&q=%22dark%20web%22 Access: November 2018.
[37] More information about it on https://www.oxforddictionaries.com/press/news/2016/9/2/WOTY Access: December 2018.

remain anonymous or untraceable,' followed by the explanation that 'whereas the term Deep Web refers to the parts of the Internet that cannot be found using search engines, Dark Web refers specifically to websites which use encryption tools to hide the identities of hosts and users of a site, often in order to facilitate illegal activities. The term has been growing in popularity in media coverage of cybercrime.'

In fact, the media approach Deep Web technologies with a mixture of fascination and a sense of complexity, translated what terms they choose to use (Aiken, 2016). As the data discussed in this chapter show, "Dark Web" has been largely the most used concept in newspapers, referring to online spaces in which users protect their identities for multiple reasons, although the British press highlight mainly negative uses. This concept is also named "Darknet" and relates to the idea of an Internet-based underworld not limited to the Tor Network but including any system in which users have freedom and anonymity to act beyond society's norms: '[I]t is dark because we rarely see it: it tends to be hidden, obscure or secret' (Bartlett, 2015, p. 3). Finally, this chapter addresses the use by British newspapers of these concepts over time, to reveal how technologies associated with the Deep Web are defined and framed by the mainstream media. Considering that these concepts are related to the construction of meaning of these technologies, and in a subsequent stage their own uses and users, this chapter discusses not only how the press struggle to define these technologies, but also the power of the language in constructing an idea of the Deep Web as something mysterious, evil and illicit.

4.2 Constructing the Dark Web

Conceptualisation is a process that involves language, which per se is social information (Spolsky, 1998), and the power of words affects the social structure in ways that are transformed over time (Koselleck, 2004). As Lakoff & Johnson (1980) insightfully show, metaphors are not only a common language resource and part of the conceptual system in which we attribute meaning to things in the world, but they are also a pervasive component of everyday realities, because they are related to concepts and terms and, on a different level, to thoughts about a specific concept and actions that are taken in reaction to it. Metaphors likewise help to guide the imaginary about a concept, according to Langer (1954, p. 113), for whom 'in a genuine metaphor,

an image of the literal meaning is our symbol for the figurative meaning, the thing that has no name of its own.'

This can be exemplified by the terms that act as the core of this research: "Deep Web" relates to content that extends far from the surface; "Dark Web" highlights the part of the Internet that has little or no light upon it; "Hidden Web" focuses on what is kept out of sight and so on. In addition, the choice of using one or another concept is not neutral but associated with specific interpretations and affects, since "Deep Web" and "Hidden Web" are related to users looking for further content or knowledge, while "Dark Web" is linked to illegal uses. Finally, metaphors are also identified in terms referring to the portion of the Internet that is easily accessible through conventional browsers: "Surface Web" uses a metaphor connected to the idea of being apparent, and "Clearnet" explores the aspect of something transparent or clean. According to Gehl & McKelvey (2019, p. 223), in the context of these technologies, 'the adjective "dark" may bring to mind illegal or immoral activity.'

In science, metaphors are a linguistic resource used to facilitate the understanding of complex topics, explained in ordinary terms 'with concepts and experiences that are familiar to their audiences' (Armon, 2017, p. 444). Some terms are often borrowed by journalists to introduce new topics to the public. In fact, metaphors help construct social representations of science and technology, which ultimately is 'an attempt to juxtapose techno scientific endeavour with everyday life activities and entities, and consequently bring it conceptually closer to non-experts; on the other hand their use could contribute to enlarge the psychological gap between S&T and the ordinary man' (Christidou et el., 2004, p. 358). In addition, in the case of novelty, 'a metaphor encourages the individual to respond to the introduction of the new technology by invoking his or her own experiences' (Williams, 2013, p. 1405).

Metaphors are also often adopted in the academic literature. Brunton (2013), for instance, refers to the 'shadow history of the Internet' when discussing the development and popularisation of spam, considered as unwanted messages largely distributed over the Web. Taking specifically the metaphor "dark," for instance, its association with ideas of mystery or negative denotations is broadly evident. An example is the concept of "dark matter," named for the first time in 1906 by the French mathematician and theoretical physicist Henri Poincaré. The

name was chosen to define the 'obscure stars which circulate in the interstellar spaces and whose existence might long remain unknown' (Poincaré, 1906, p. 480), after the discovery by the mathematical physicist Lorde Kelvin that only stars that emit light can be observed from Earth. In this case, "dark" is translated to what is unknown in the Universe. Another example of a metaphor used in science is the Black Box Theory, explained by the pioneer of cybernetics Ashby (1956, p. vi) as 'the case when the system is such that not all of it is accessible to direct observation.' Nowadays, this term is informally adopted by people who do not understand how a technology works; for instance, a smartphone can be viewed as a "black box." There are examples also in popular culture. A true fan of the *Star Wars* franchise[38] will know that the Dark Side of the Force is connected to the evil use of the power of the Galaxy. In fact, its best-known symbol is Darth Vader[39] – the literal translation "Dark Father" –, the villain who wears dark clothes, has his face covered with a dark mask and an unrecognisable voice and plots to destroy the Jedi Order, which represents the balanced use of the power in the Universe.

In fact, the antagonism of "light" and "darkness" to refer to the ideas of good and bad is not a tool used purely by the media (Forceville & Renckens, 2013). Osborn (1967), for instance, debates this opposition in Winston Churchill's war speeches, not only as metaphors for conflict and peace, but also related to the idea of night and day as inevitably subsequent things; in this logic, peace is a result of the war. Mommsen (1942) argues about the concept of the Dark Ages, often used to refer to the Middle Ages, a period between the fifth and the fifteenth centuries commonly known for the lack of intellectual progress. In a completely distinct setting, Schlosser (2012) refers to fast-food chains as the dark side of nourishment.

On the matter of the metaphor "Deep Web," it is often related to the analogy of an iceberg widely used to explain these systems: looking for this term in Google Images[40] results in several pictures of icebergs (see Figure 12). In this metaphor, everything that is over the water line, and

[38] More information about the movies on https://www.starwars.com. Access: December 2019.
[39] More information about the character on https://www.starwars.com/databank/darth-vader. Access: December 2019.
[40] Available on https://www.google.co.uk/search?q=deep+web&rlz=1C5CHFA_enGB749GB749&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi3wZ6elcDeAhVsB8AKHSbwC4sQ_AUIDigB&biw=1280&bih=595 Access: October 2019.

therefore visible, is the Surface Web, and everything that is under the water line is the Deep Web, requiring the user to dive down in order to gain access to its content. Using the metaphor of the ocean to explain content on the Internet is not uncommon: as a matter of fact, a usual synonym for online "browsing" is the term "navigating."

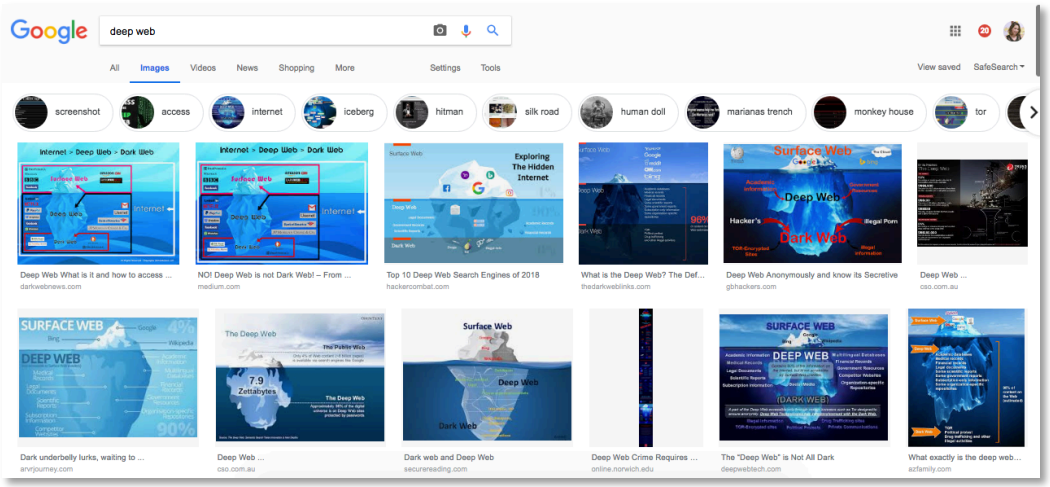


Figure 12: Search for the term "Deep Web" in Google Images
Source: Google Images
Retrieved by the author in October 2019

Contemplating the relevance of metaphors to indicate how technologies are represented, and the fact that the Deep Web can be named in multiple ways – as seen through the terms used not only in the academic literature, but also by the public in everyday life searches on Google –, this research looks at newspapers to conclude that the commonest metaphor associated with these technologies in the British press is "dark." This attribute is used in 77.3% of the headlines, when considering 159 headlines from the six newspapers that nominally mention these technologies and in 91.6% of the articles, from a total of 833 publications. Variations of this metaphor include the terms "Dark Web," "Darknet," "Dark Side" and "Dark Internet."

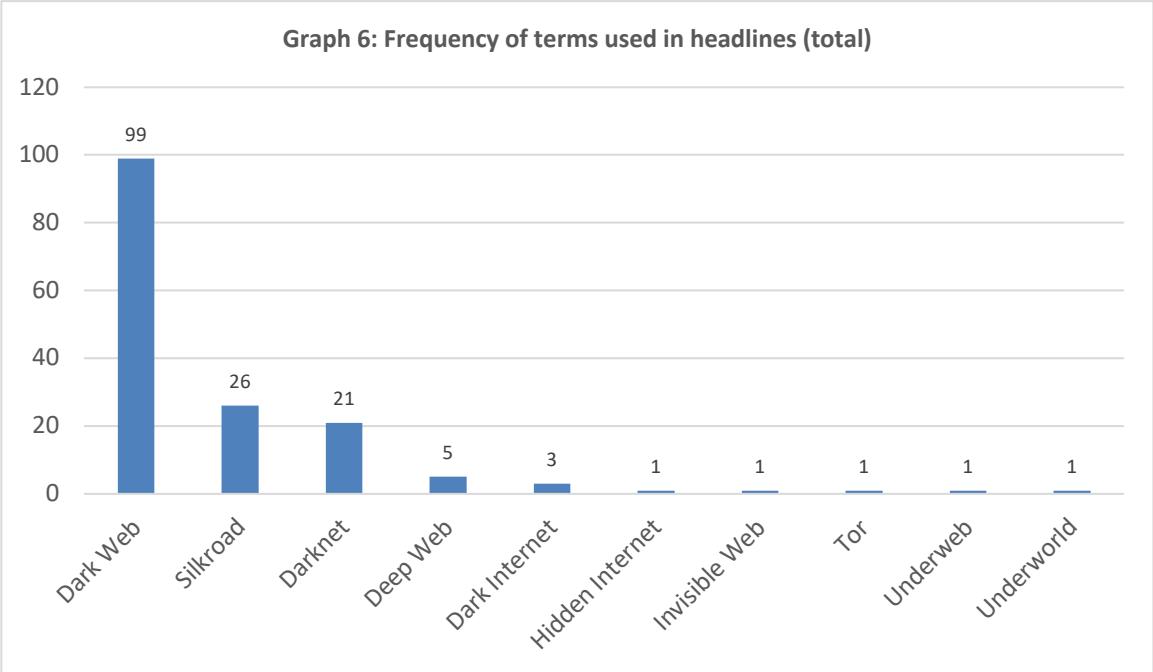
Since the use of the attribute "dark" is constantly connected to negative uses (Mommsen, 1942; Osborn, 1967; Schlosser, 2012; Forceville & Renckens, 2013), it is not a surprise that the first time it was used to name Deep Web technologies, among the six researched newspapers,

was in an article published by the *Daily Mirror*[41] in August 2005 strongly criticising the existence of Freenet:

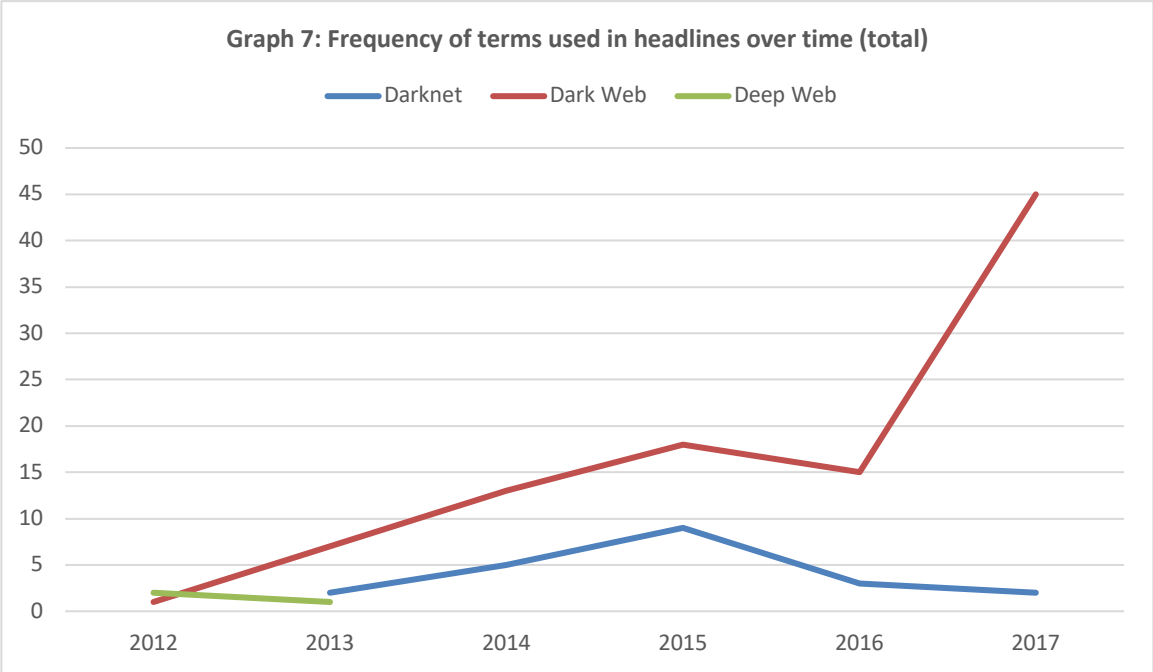
```
Ian Clarke, 28, from Navan, Co Meath, is set to launch his revolutionary on the
Freenet software this Christmas, which will allow users to hide their identity
internet and share information anonymously. But experts fear that terrorists
might use Freenet to communicate with each other, safe in the knowledge that no
one will know what they are up to. It's thought the software could also be
abused by paedophiles and hackers. America's Senate Commerce Committee has
called on the US government to legislate against "dark-net" technology.
```

As studies in Journalism show, headlines have purposes of giving an overall picture of the content and attracting readers, which leads to a questionable use of attention-getting words (Reah, 2002). In fact, headlines have the persuasive function of not only establishing the general view of a newspaper about a topic, but also manipulating and influencing opinions through the choice of words and which aspects are emphasised or not (Reah, 2002. For what concerns headlines analysed in the research, the preference for using the attribute "dark" is evident: in a total of 159 cases in which newspapers used a concept in headlines, this attribute was chosen 123 times (Graph 6).

[41] Related article: "Fears over Irish web invention," Daily Mirror, 14th August 2005, News, page 2.



Considering the use of these concepts over time, the establishment of a trend in headlines is also clear. It is worth reminding the reader that this research collected every article from six British newspapers mentioning 27 keywords related to Deep Web technologies, from the first occurrence in 2001 through to 2017, as explained in the *Methodological Framework*, but the articles were rare at the start, and only from 2013 did news on the topic see a substantial increase in numbers. Considering that articles about this technology were not frequent in the media, the term "Deep Web" occurred more often than any other in 2012 (Graph 7). After 2013, however, "Deep Web" was never mentioned again in headlines, so the lifetime of this concept was brief in the newspaper context. Although the term "Darknet" was present in headlines from 2013, consistently growing until 2015 and declining thereafter, it also was never largely adopted by the British press.



The choice to use the term "Dark Web" in newspaper headlines is undeniable. Since 2012, the numbers of occurrences have consistently grown every year (2016 looks like an exception at first sight, but it was a year in which the overall number of articles about this topic was lower). In fact, "Dark Web" or "Darknet," which are used interchangeably, since both apply the same metaphor of "dark," are the preferred terms and have the same tendency of use, but in 2017 the term "Dark Web" established clear dominance, as it was used 45 times out of 47 cases. Considering that newspapers propose an understanding of the news through headlines (Bignell, 2002), and the important role of metaphors in defining and directing meaning (Lakoff & Johnson, 1980), British print media are framing this technology through an obscure – dark, with no light – meaning. Moreover, the fact that popular newspapers more obviously frame everyday life situations in a negative and sensational way (Conboy, 2006) is clear when comparing how tabloid and quality newspapers utilise these terms. To show how this occurs in the researched newspapers, this work compares the use of attributes mentioned in headlines, grouping distinct terms that recur in relation to the same metaphor (as seen in Table 8).

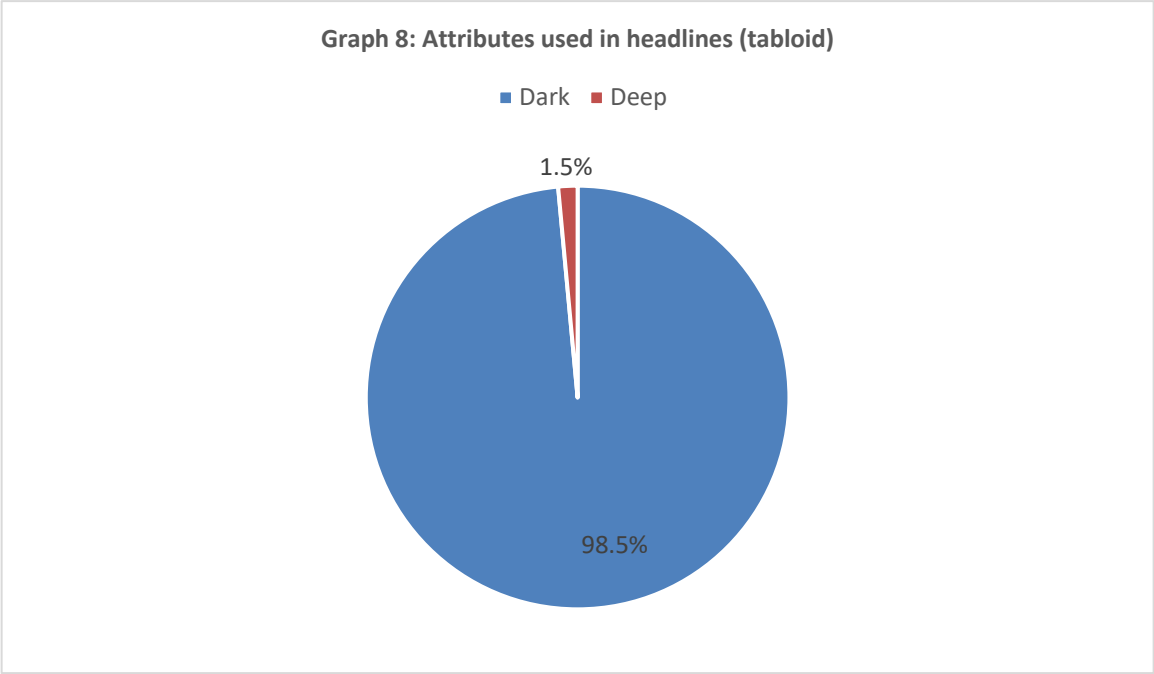
Table 8: Concepts used to define the Deep Web, based on attributes

ATTRIBUTE	CONCEPT
Dark	Dark Internet Darknet Dark Web Dark side
Deep	Deep Internet Deep Net Deep Web
Under	Undernet Underweb Underworld
Hidden	Hidden Internet Hidden Web
Invisible	Invisible Internet Invisible web

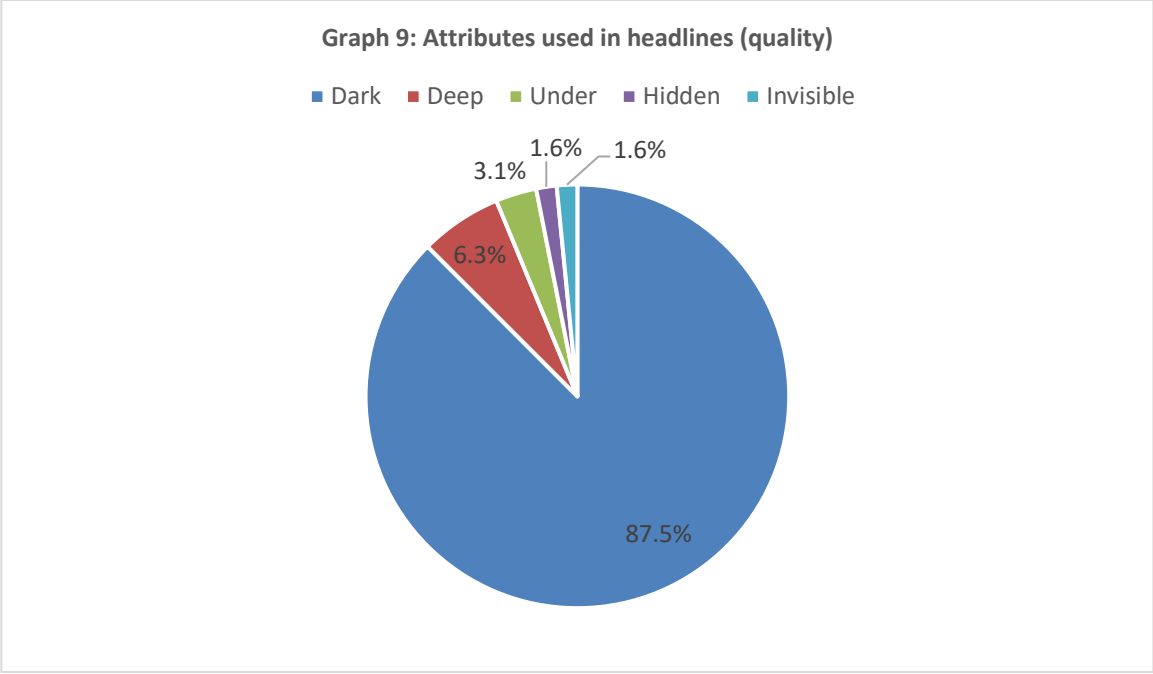
Including the variations "Dark Internet," "Darknet," "Dark Web" and "Dark side," the attribute "dark" is responsible for 98.5% of the cases in the tabloids (Graph 8). Actually, the attribute "deep" was used only once by tabloids in headlines, a total of 1.5%. The case is the article "Drugs, guns, assassins, jet planes… All for sale on secret Deep Web,"[42] published by *Daily Mirror* in September 2012. Although the use of the attribute "deep" instead of "dark" could possibly indicate a more neutral approach to the topic, the article in question can be summarised as a strong statement against the Deep Web, which reduces all content outside of traditional search engines and browsers to crypto markets trading drugs, documents and child pornography, among other illicit uses. In fact, the same article even mentions that:

```
1 | Internet can be scary but what lurks beneath is terrifying.
```

[42] Related article: "Drugs, guns, assassins, jet planes… All for sale on secret Deep Web," Daily Mirror, 22nd September 2012, News, page 18.



In quality newspapers (Graph 9), although there is more variety in relation to attributes – including those shown in Table 8 – the same preference for "dark" seen in tabloids is also underlined by its occurrence in 87.5% of the headlines. This means that the attribute "dark" was used 56 times and the others, combined, only eight times.



The use of the attribute "invisible" in quality newspaper headlines, nevertheless, was rare: it happened only once and in the very early stages of the media addressing this topic in an article published by *The Guardian* in September 2001 and entitled "Search for the invisible web: There are more websites than those seen with the naked eye,"[43] in which the author explains how thousands of databases are hidden from mainstream search engines. The attribute "hidden" is also rarely applied by quality newspapers, and an example of this use comes from *The Times* with the article "Unsafety Net: The Policing of the hidden internet cannot be left to vigilantes,"[44] published in May 2017. Interestingly enough, the same article applies the term "darknet" in the text. Although there is a strong preference for associating these systems with the sinister idea the attribute "dark" connotes in headlines of both tabloids and quality newspapers, the use of concepts in the text of the article shows a wider representation of these systems. Although the articles also prefer the term "Dark Web," in 58.0% of the cases, many terms are included in the text but ignored in headlines (Graph 10), i.e. newspapers use 18 different concepts in the text, compared to 10 in the headlines. Some of these concepts were mentioned only once in the texts, though. An example is "Undernet," used by *The Guardian*[45] in October 2008 when comparing the Surface and Deep Web:

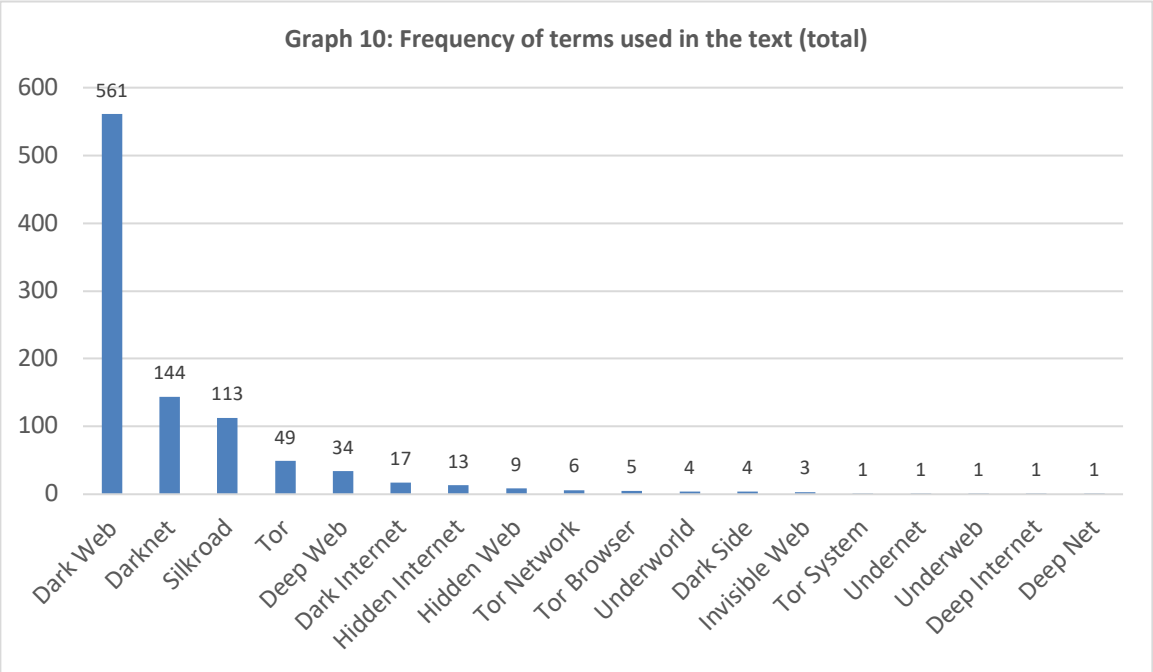
```
A trusted, controlled 'overnet' for commercial and business use, and an
'undernet' where anything goes.
```

It is also the case for "Underweb," which was applied also by *The Guardian*[46] in November 2002:

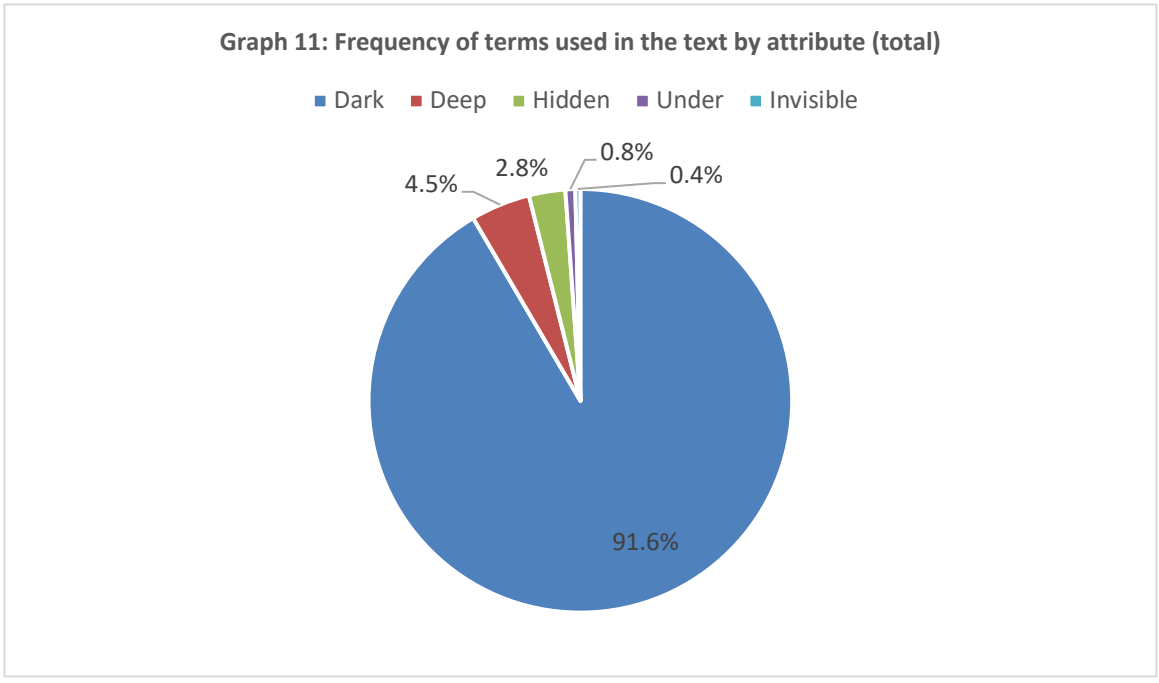
```
Other sites, part of what Leach calls the 'underweb,' will go to great lengths
```

[43] Related article: "Search for the invisible web: There are more websites than those seen with the naked eye," The Guardian, 6th September 2001, Guardian Online Pages, page 1.
[44] Related article: "Unsafety Net: The Policing of the hidden internet cannot be left to vigilantes," The Times, 8th May 2017, Editorial, page 21.
[45] Related article: "It's every man for himself," The Guardian, 2nd October 2008, Guardian Technology Pages, page 1.
[46] Related article: "Shop tactics: Counter culture," The Guardian, 28th November 2002, Guardian Online Pages, page 2.

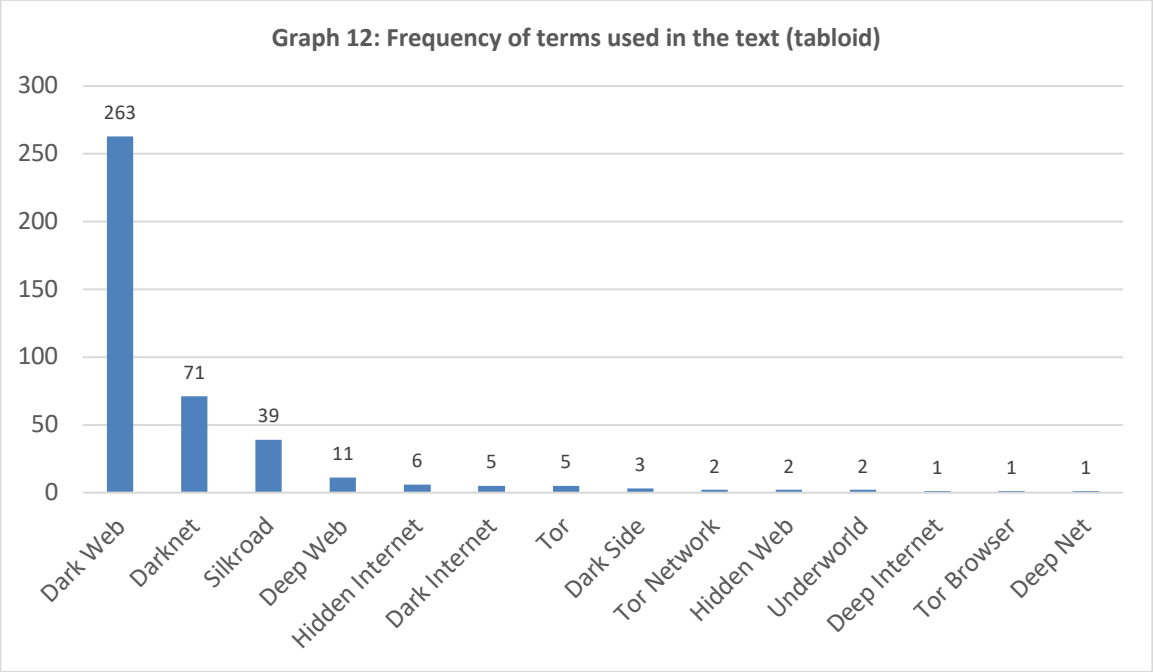
2 to ensure they are not found by uninvited guests.

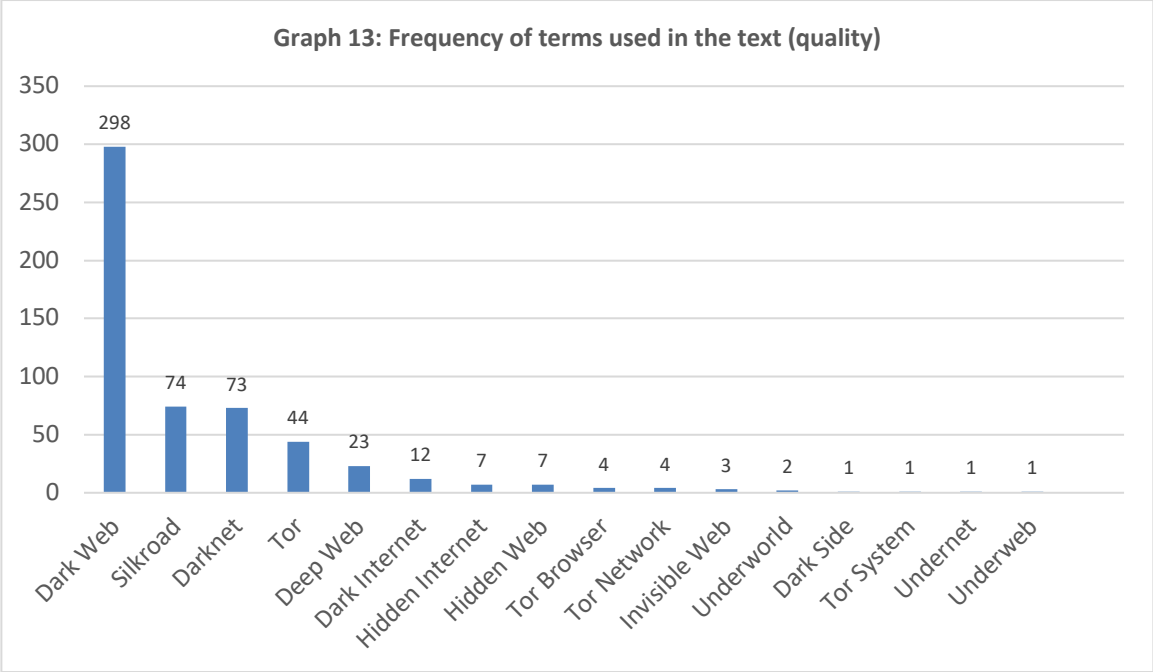


Considering the use of attributes (as seen in Table 8), the pattern is actually still consistent with the headlines, with the choice of the attribute “dark” in 91.6% of the cases (see Graph 11).



The preference for the concepts “Dark Web” and “Darknet” in the text of the articles is clear, as seen in Graphs 12 and 13, which show tabloid and quality newspapers separately.





The third most used term in the articles, with a total of 39 appearances, "Silk Road," deserves special discussion. First, "Silk Road" in this case relates to a crypto market mainly known for commerce in drugs, and it is a metaphor related to the actual Silk Road[47], the millennial network of routes connecting Asia and Europe. This road was developed over two thousand years ago for the purpose of trading Chinese silk, but it was also used for the exchange of other goods and even knowledge and ideas among Asian and European cultures over time. In the case of the crypto market, users from distinct countries were connected, thereby allowing illegal substances to cross borders and circulate between continents through the postal service. Second in this regard, a metaphor is commonly used by newspapers to define this website when calling it "eBay for drugs," in reference to the e-commerce which facilitates consumer-to-consumer and business-to-consumer trades, or the variation "Amazon.com for drugs," also in reference to an e-commerce website. In April 2012, for instance, *The Times* article[48] mentioned:

```
1 |    The site, called Silk Road, is an Amazon.com for illicit material.
```

It is noteworthy that Aldridge & Décary-Hétu (2014) point out that comparing it to eBay or Amazon is inaccurate: after an extant analysis of transactions, it was concluded that most of the trade on Silk Road is actually business-to-business , with a recognised flow from big drug dealers to local street sellers. Nevertheless, In October 2013, *The Guardian* article[49] referred to:

```
1 | A version of eBay for drug dealing: matching buyers and sellers of different
2 | substances.
```

In summary, the findings convincingly show that although newspapers in the United Kingdom have neutral alternatives available, they deliberately adopt terms that are conceptually related to the negative uses of privacy-enhancing technologies, with little difference between tabloids and quality newspapers. As a sharp example of this, the term "Dark Web" was the most common

[47] More information on https://en.unesco.org/Silk Road/ Access: January 2019.
[48] Related article: "It's like Amazon, but for criminals," The Times, 3rd April 2012, Features, page 40.
[49] Related article: "Alleged owner of Silk Road drug website seized in US," The Guardian, 3rd October 2013, Guardian Home Pages, page 6.

choice for journalists discussing the phenomenon over time, which suggests an overwhelmingly negative representation of these technologies in the British press.

4.3 2015: The Year in which Readers learnt what the Dark Web is

The media and the scientific community have distinct approaches when introducing new ideas and developments to the public, for instance when presenting new concepts. In fact, scientists often 'blame the media for sensationalism, inaccuracy and distortion' (Haran & Kitzinger, 2009, p. 634). Considering this point, this work examines definitions of the Deep Web provided by newspapers in an aim to discuss the ways in which these technologies are framed. In this context, this research considers how the article explains and clarifies what not only some concept, idea or object may be, but also the general assumption behind the use of a definition that implies the public lacks that knowledge. When smartphones, for instance, were still a novelty in the previous decade, the media would generally explain how the combination of a telephone, a computer and the Internet was promoting a revolution in personal digital communication (Miller, 2014). Nowadays, however, the media no longer include definitions in their stories; instead, due to these devices' extended diffusion, articles about the topic take for granted that the public knows what a smartphone is. The earliest discussions of a new technology or system, in this sense, provide interesting insights into the initial terms through which it is understood and interpreted in the public sphere.

In the case of Deep Web technologies, it is noteworthy to see how each of the researched newspapers introduced this concept for the first time. Starting with the tabloids, *The Sun*[50] gives a brief explanation in August 2010, focusing on a technical aspect of the system and size, stating that:

```
1 Now firms are offering to trawl the 'deep web' and manage your reputation
2 online. More than 90 per cent of the internet is not searchable by Google.
```

[50] Related article: "Internet repair kit," The Sun, 14th August 2010, News, page 22.

In a *Daily Mail*[51] article from 2012, the Deep Internet is defined as:

```
An anonymous network which is even tougher for the police to trace and requires
you to download special programs.
```

This shows a security point of view, combining technical information and the threat represented by anonymity. *Daily Mirror*[52] discusses in 2015 the software element, highlighting also fear over the tool's potential for protecting identities:

```
Which will allow users to hide their identity on the internet and share
information anonymously.
```

In the quality newspapers, however, the first definition used in each of the newspapers focuses on technical information and available content, with no mentions of security or anonymity. Starting with *The Guardian*[53] in 2001, the article defines the Invisible Web on a technical level:

```
Invisible Web is made up of information that search engines either cannot or
will not add to their web indexes.
```

In *The Times*[54], the Deep Web was defined in 2004 according to the extent of content:

```
The vast tracts of information – estimated at more than 500 times more than can
be found on the readily accessible, or 'surface,' web – stored in digital
archives that today's browsers never peek into.
```

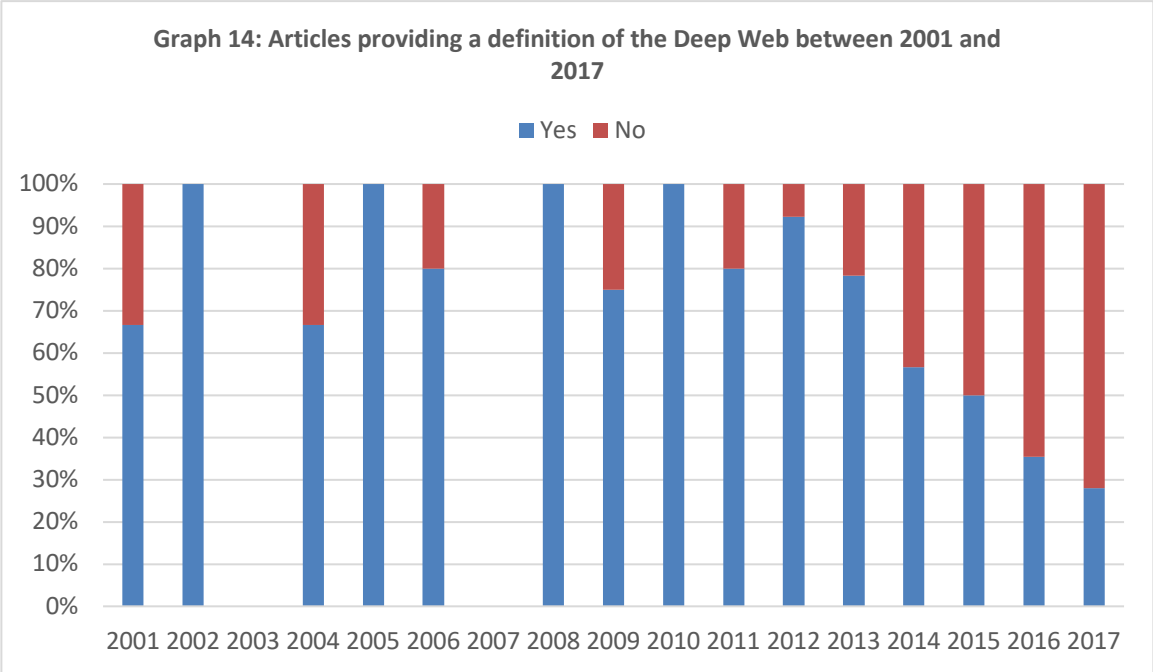
Finally, in 2006, also focusing on content, *Daily Telegraph*[55] assures that the Deep Web:

[51] Related article: "Sold for £19: your credit card details," Daily Mail, 8th February 2012.
[52] Related article: "Fears over Irish web invention," Daily Mirror, 14th August 2015, News, page 2.
[53] Related article: "Search for the invisible web," The Guardian, 6th September 2001, Guardian Online Pages, page 1.
[54] Related article: "Connected, or confused?," The Times, 24th June 2004, Features, page 12.
[55] Related article: "How to dig deeper: Voyage to the bottom of the internet," The Daily Telegraph, 7th October 2006, Art, page 20.

```
Exists in archives, databases, catalogues, private and secure websites and as
non-standard or 'dynamic' pages that are created in response to specific
enquiries.
```

The distinction between quality and tabloid approaches when first defining these systems can be partially explained according to the year of publication. In the case of quality newspapers, the topic was addressed when there was little information about criminal uses of Deep Web systems – *The Guardian* in 2001, *The Times* in 2004 and *The Daily Telegraph* in 2006. In the case of tabloids, however, coverage on the topic came much later – *The Sun* in 2010, *Daily Mail* in 2012 and *Daily Mirror* in 2015 – with discussions discussing the security aspect of these technologies, which were already established. This may exemplify, however, that the interest of these newspapers in these technologies is mainly related to negative uses and crime coverage, a topic that is discussed in depth in the next chapter.

In recent examples, British newspapers still include definitions of this technology, an indication that the authors believe the public needs an explanation about how it works. Among the findings of this research, articles present definitions of Deep Web technologies in 46.2% of the publications. As seen in Graph 14, from 2001 to 2011, years in which the number of articles was never over 10, which hinders the analysis of the newspapers' behaviour, the percentage of articles with a definition was always superior to those without one.

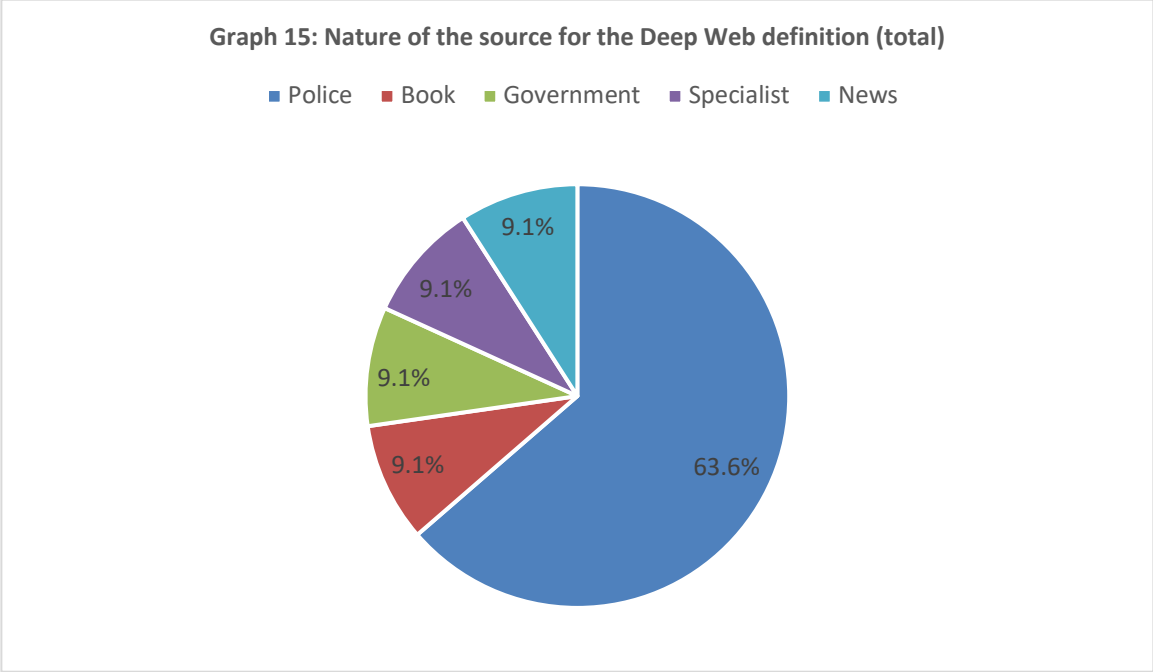


Nevertheless, according to Graph 14, the percentage of articles providing a definition for Deep Web technologies from the total number of publications consistently decreased from2012. In fact, the proportion of articles presenting a definition in 2012 was 92.3%; after that, 78.3% in 2013; 56.6% in 2014; 50.0% in 2015; 35.3% in 2016 and, finally, 28.0% in 2017. As the graph shows, 2015 was the first year in which cases of using a definition equalled those not using a definition, and from that point on, publications without definitions were in the majority. More recently, however, definitions are often used in an extremely simplified and direct way, usually highlighting the security or technical aspects of accessing these technologies. In recent examples from 2017, newspaper articles very briefly explain what constitutes the Dark Web:

Daily Mail	The secretive area of the internet often exploited by criminals.
The Sun	An encrypted corner of the internet that can only be accessed by special browsers
The Times	The hard-to-access online network often used by criminals.

Although definitions are present in 46.2% of the cases, newspapers tend to ignore the origin of these definitions, such as an information source. In fact, the source is mentioned only 11 times, and it is worth remembering there are 385 cases in which newspapers present a definition from

a total of 833 articles making up part of the analysis. While Brown et al. (1987) remind us that there is an invisible power played by the media related to sources in articles, since the plurality of viewpoints is an essential dimension of democracy, in practice there is a heavy use of official sources such as members of police or governmental institutions. This is easily identifiable in this research, in that police sources are apparent in 63.6% of cases (Graph 15).



Considering the rare nature of the presence of the source explaining the Deep Web, the fact that the most recurrent one is the police, instead of academics or IT professionals connected to technology studies and/or development, also shows a bias towards the negative representation of these technologies. This is the case, for instance, in the article published by the *Daily Telegraph*[56] in December 2013, whereby the explanation about Silk Road has as its source the Federal Bureau of Investigation (FBI):

```
1 The agency damned Silk Road as 'the most sophisticated and extensive criminal
2 marketplace on the internet.'
```

[56] Related article: "Bitcoin is threat to the power of central banks," Daily Telegraph, 17th December 2013, Business, page 4.

In this specific case, moreover, the use of the term “damned” adds a layer of criminality to the technology. Altogether, these choices are part of the process of representation made through media and cultural industries, and they create the meaning and establish common sense while normalising ideas related to a concept, an object or an idea (Kidd, 2016). Ultimately, the lack of definitions, the considerable absence of sources, and the use of official sources such as police that emphasises only the security dimension of the Deep Web, surely contributes to the sharply negative representation of these technologies made by British print media.

4.4 “Hidden,” “encrypted,” “secretive”: too many Attributes

Whilst human imagination plays a role in the understanding and use of machines and technology (Natale & Balbi, 2014), and communication outlets have a fundamental effect on the way society perceives the world, with political, historical and social implications (Kidd, 2016), the media as an institution have the power not only to inform how things in the world are represented, but also to influence their uses. In this context, the concepts used to refer to Deep Web technologies, and the language used to define them, are relevant in guiding this representation and potential use.

Table 9 presents a list of 70 attributes, organised in alphabetical order, used by newspapers in their definitions of Deep Web technologies. It is relevant to review two points previously mentioned in the *Methodological Framework*. First, this research collected only the first name or adjective used in the definition of these technologies delivered by the article, and second, this research uses the general expression “attributes” to refer to these names and adjectives. Among the data, there are attributes highlighting distinct aspects of these technologies; for instance, “anonymous” focuses on the fact that users can hide their identities, “encrypted” is connected to the technical dimension and the layers of protection against online surveillance, “secretive” underlines the mystery that surrounds these systems and so on.

Table 9: Occurrences of attributes associated with Deep Web technologies by newspaper

	NEWSPAPER						TOTAL
	DAILY MAIL	DAILY MIRROR	THE GUARDIAN	DAILY TELEGRAPH	THE SUN	THE TIMES	
Abnormal	0	0	0	0	1	0	1
Anonymous	4	1	6	0	3	9	23
Bazaar	0	0	0	2	0	0	2
Black-market	0	6	3	2	2	4	17
Booming	1	0	1	0	0	0	2
Buried	0	0	1	0	1	0	2
Chaotic	0	0	0	0	0	1	1
Chilling	0	1	0	0	0	0	1
Complex	0	0	1	1	0	0	2
Comprehensive	0	0	1	0	0	0	1
Covert	0	0	0	0	1	1	2
Criminal	1	1	4	0	0	6	12
Dark	0	0	1	1	0	0	2
Difficult	0	1	0	1	0	0	2
Dodgy	0	1	0	0	0	0	1
Drug-dealing	0	1	0	0	0	0	1
Encrypted	13	2	4	7	7	7	40
Free	0	0	1	0	0	0	1
Grey	0	0	1	0	0	0	1
Grim	0	0	0	0	1	0	1

Harder	2	0	0	1	0	1	4
Hidden	13	12	9	3	7	21	65
Huge	0	0	1	0	0	0	1
Illegal	3	3	2	0	4	2	14
Illicit	4	1	2	0	1	2	10
Inaccessible	2	0	0	0	0	1	3
Infamous	0	0	0	1	0	0	1
Interesting	0	0	1	0	0	0	1
Invisible	1	1	0	1	1	3	7
Large	0	0	0	1	0	0	1
Lawless	0	1	1	1	1	2	6
Major	0	0	0	0	0	1	1
Murky	2	0	0	1	1	0	4
Mysterious	0	0	0	0	0	1	1
Nasty	0	1	0	0	0	0	1
Not indexed	0	0	0	0	0	1	1
Not viewable	0	0	0	0	1	0	1
Notorious	4	0	1	2	1	1	9
Noxious	1	0	0	0	0	1	2
Parallel	1	0	1	0	0	0	2
Popular	0	0	1	0	0	0	1
Private	0	0	0	0	0	2	2
Refuge	1	0	0	0	0	1	2
Resilient	0	0	1	0	0	0	1

Restricted	1	0	1	0	0	1	3
Route	1	0	0	0	0	0	1
Safe	0	0	1	0	0	0	1
Secretive	10	6	5	1	10	4	36
Secure	0	0	2	0	0	1	3
Shadowy	3	2	1	1	7	2	16
Shield	0	0	1	0	0	0	1
Sick	0	2	0	0	0	0	2
Sinister	0	1	1	1	3	3	9
Solution	0	0	1	0	0	0	1
Sophisticated	0	1	1	1	1	3	7
Specialised	0	1	2	4	2	9	18
Treasure	0	0	1	0	0	0	1
Ugly	0	1	0	0	0	0	1
Uncharted	0	0	1	0	0	0	1
Under the radar	0	1	0	1	0	0	2
Underground	0	3	5	1	3	6	18
Underside	0	0	0	1	0	1	2
Undetectable	1	0	0	0	0	0	1
Unlisted	0	2	0	0	0	0	2
Unpoliced	1	0	0	1	0	1	3
Unreachable	0	1	1	0	0	0	2
Unregulated	4	0	0	0	0	2	6

Untraceable	3	1	2	0	0	3	9
Vast	0	1	0	0	0	1	2
Vile	0	0	0	0	0	1	1

As this table shows, the most common attribute associated with these technologies and used by newspapers is the term "hidden," with 65 occurrences, a word related to things that are not easy to find, deliberately taken from the view or that people do not know about. The first time that this attribute was applied was by *The Guardian*[57] in November 2009. In the article, there is a script of how to access these systems, with the aim to:

```
Enter a previously hidden online world.
```

Since then, this attribute has been commonly used: in December 2017, for instance, *Daily Mirror*[58] pointed it out when defining these technologies, as the following extract shows:

```
Grant West, 25, hacked the online fast food giant (Just Eat) and firms
including Uber, Sainsbury's and Argos for data flog on the 'dark web,' a hidden
part of the internet used by criminals.
```

Fascinatingly, these examples point to different perspectives of the same attribute: in the case of *The Guardian*, "hidden" is used to attract curiosity about the content, and in the case of *Daily Mirror*, it can be translated as a hideout for felons. Considering each newspaper separately, the most used attributes are "hidden," with 21 cases in *The Times*, 12 cases in *Daily Mirror* and nine cases in *The Guardian*; "hidden" and "encrypted," both with 13 cases each, by *Daily Mail*; "encrypted" with seven cases in *Daily Telegraph* and "secretive" with 10 cases by *The Sun*. Although these attributes highlight distinct dimensions, they all contribute to the general idea of the Deep Web as something unknown, secret and inaccessible, giving opacity to these

[57] Related article: "A walk on the darkside: A tiny fraction of everything online can be found via search engine," The Guardian, 26th November 2009, Guardian Features Pages, page 4.
[58] Related article: "Just Eat data crook in dock," Daily Mirror, 15th December 2017, News, page 28.

technologies. There are multiple forms of accrediting a dimension of opacity to technologies (Burrell, 2016), such as stressing an intentional element secrecy in the technology's development, highlighting digital illiteracy, and therefore lack of knowledge about how that technology works, discussing the uses in itself and others. The fact that the British press favour the opacity of the Deep Web becomes clearer when grouping the previously mentioned attributes by topic (as seen in Table 10).

Table 10: Attributes used by newspapers by topic

TOPIC	ATTRIBUTES
Anonymity	Anonymous
Trade	Bazaar Black-market
Technology	Complex Encrypted Inaccessible Not indexed Restricted Route Safe Sophisticated Specialised
Legality	Illegal Illicit Lawless Unpoliced Unregulated
Relevance	Comprehensive Interesting New phenomenon Notorious Popular Resilient Treasure

Size	Booming Huge Large Major Vast
Criminality	Abnormal Chilling Criminal Dodgy Drug-dealing Evil Grey Grim Infamous Nasty Noxious Sick Ugly Vile
Secrecy	Buried Chaotic Dark Harder Hidden Invisible Murky Mysterious Not viewable Parallel Secretive Shadowy Sinister Uncharted Underground Underside Unlisted Wonderland
Counter surveillance	Covert Difficult

```
Free
Private
Refuge
Secure
Shield
Solution
Under the radar
Undetectable
Unreachable
Untraceable
```

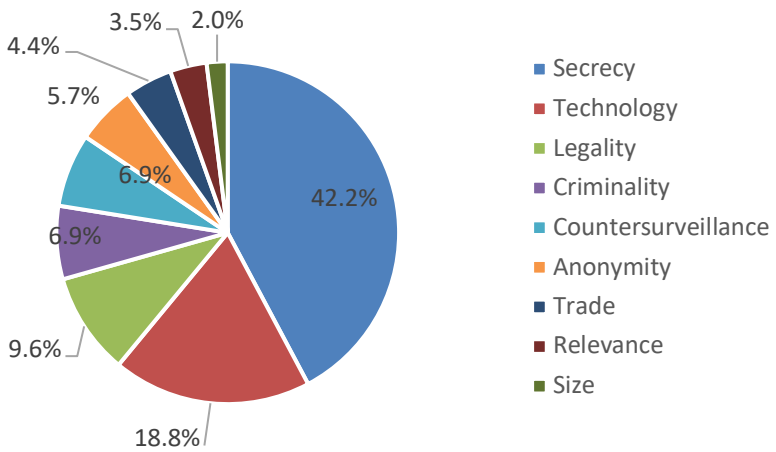
First, the table shows that most of the attributes used in these cases are neutral – for instance, “anonymous” and “restricted” – or negative – in the cases of “criminal” and “sinister.” In opposition, rare examples of positive ones occur, such as “solution,” used by *The Guardian*[59] in April 2012:

```
1 The Tor Browser and software obfuscates a user's web traffic so anyone watching
2 is unable to trace who a user is or where they are coming from. This is a
3 technological solution to what Lewman feels is an elemental problem. 'The
4 ability to forget, to start over is important,’ he argues.
```

In this case, the article is a relevant discussion about privacy and the freedom of anonymity, and the negative potential use of Tor is not the focus of the text. Second, when looking at the above-mentioned attributes organised by topic (Graph 16), words connected with an idea of secrecy, and therefore attributing opacity to the technology (Burrell, 2016), are the majority in British newspapers, namely 42.2% of the articles. Associating a dimension of mystery to the Deep Web, newspapers not only instigate the curiosity of the readers, but they also shape their perceptions of these technologies through an image of the supernatural or extraordinary.

[59] Related article: "Is it more important to have a single persona or the freedom of anonymity?” The Guardian, 20th April 2012, Guardian Home Pages, page 19.

Graph 16: Attributes used in newspaper articles by nature (total)



Newspapers underline the technical aspects of the Deep Web in 18.8% of the cases, which can also contribute to the opacity surrounding the Deep Web, since the meaning of attributes such as "encrypted" is not largely known by the general public and demands a level of knowledge in technology (Gehl, 2016). This attribute is used, for instance, to add a layer of sophistication to the technology and justify governmental action against it. As an example, an article published by *Daily Mail*[60] mentions that:

```
Britain's spy agencies are to be brought in to try to smash the dark web used
by paedophiles to share vile images and videos. GCHQ will try to identity
thousands of the most sophisticated child abusers who use encrypted internet
networks.
```

Fascinatingly, considering that the main reason for Tor's existence is to provide online privacy, newspapers highlight the relevance of these technologies in avoiding surveillance only in 6.9% of cases, using attributes such as "untraceable" and "undetected." Yet, pointing to the problem of surveillance does not imply that privacy-enhancing technologies are represented

[60] Related article: "GCHQ spies bid to tackle Dark Web," Daily Mail, 19th November 2013.

positively. When a newspaper focuses on the fact that the users cannot be traced while using Tor, there is a preoccupation related to how this is used by criminals to avoid persecution. The attribute "untraceable," for instance, is used by *The Times*[61] in September 2014 in the following:

```
Miss Patel had bought abrin, a controlled substance under the Terrorism Act,
from an illegal website called Black Market Reloaded (BMR) in the US using
untraceable software and £900 of bitcoins.
```

This example shows how the idea of being beyond the authority's radar is commonly associated with crimes, as the next chapter explores in depth. On the one hand, newspaper articles consistently repeat attributes that are related to neutral or negative aspects of the Deep Web, with little space for positive perspectives. And on the other hand, even when the attributes are not negative per se, they constantly give opacity to these systems, increasing the distance between the technology – which has well-known positive uses (Baek et al., 2016; Bellare & Rogaway, 2005; Dingledine et al., 2004; Floridi, 2014; Hoang & Pishva, 2014; Jardine, 2018a; Kendrick, 2007; Pedley, 2002; Sharon & John, 2018; Su, 2008; Sui et al., 2015; Theng et al., 2016; van Baalen, 2018; Wu & Atkin, 2018) – and regular Internet users.

4.5 Discussion: Negative, Inexplicable and Opaque

The media play a central role when a new technology is introduced to the public, because the technology portrayal in the press and via other media platforms enables the construction of meaning (Carpentier, 2011; Durham & Kellner, 2006; Taylor, 2014) in the public sphere (Habermas, 2006) and affects uses (Gitelman & Pingree, 2003; Krippendorf, 2013; Mansell, 2012) in both social and cultural dimensions (Natale & Balbi, 2014). Moreover, the Web usually stimulates multiple reactions, including dreams and nightmares (Malbreil, 2007), hopes and fears (Natale & Ballatore, 2014; Sturken et al., 2004), positive and negative views (Barney et al., 2016; Bartlett, 2015; Coleman, 2014) and euphoria to resistance (Paulus et al., 2013). This work shows,

[61] Related article: "Woman forbidden from marrying 'tried to poison her evil mother,'" The Times, 23rd September 2014, News, page 5.

however, that readers of the more popular British newspapers have little or no knowledge, depending on which title they choose in everyday life, that the Deep Web has both positive and negative uses (Jardine, 2018b; Moore & Rid, 2016). As this chapter conclusively shows, British press coverage massively focuses on the negative implications of these technologies and undesirable associations, which contributes to vilifying the Deep Web.

Media representation is constructed by language (Bignell, 2002) in terms of persuasion (Kidd, 2016), ideology (Melton, 1996) and power (Orgad, 2012), and therefore analysing news content unveils meaning (Hall, 2013). Considering that this can be achieved through the use of concepts (Bolton, 1997; Loocke, 1999; Spolsky, 1998) and metaphors (Langer, 1954), the selection of terms used to describe the Deep Web helps to understand the meanings that newspapers attribute to these technologies. In fact, the British press adopt concepts that apply negative metaphors: the term "Dark Web" is consistently used by newspapers while there are neutral ones available, such as "Deep Web" or "Hidden Web." This shows a clear inclination toward terms that conceptually give negative impressions of privacy-enhancing technologies. While the academic literature generally acknowledges a distinction between the Dark Web and the Deep Web (Bartlett, 2015; Bradbury, 2014), this analysis shows that these terms are used interchangeably in the British press. An example is provided by *The Times* in the article "Unsafety Net: The Policing of the hidden internet cannot be left to vigilantes,"[62] published in May 2017, in that while the headline uses the term "hidden internet," the term "darknet" is applied in the text, with the same meaning, demonstrating the struggles newspapers find in differentiating between these concepts.

In addition, the emergence of the term "Dark Web," a concept that is per se linked to illegalities and immoralities (Gehl & McKelvey, 2019), can be contextualised within a broader shift in the overall representations of the Web, from a situation in which it was presented as a harbinger of positive change (Mosco, 2004) to a more balanced view. Although affirmative ideas of the Web were prevalent during the initial narrative (Flichy, 2007; Mosco, 2004; Streeter, 2011), discussions about the Dark Web and its overall undesirable uses show that there is a more nuanced portrayal involving both positive and negative visions of these technologies (Brunton,

[62] Related article: "Unsafety Net: The Policing of the hidden internet cannot be left to vigilantes," The Times, 8th May 2017, Editorial, page 21.

2013; Greenwald, 2014; Landau, 2017; Striphas, 2015; Van Dijck, 2013; Vargo et al., 2018). Moreover, this emergence is what Simonson (2014) calls 'rhetorical invention,' related to a sociocultural process in which novelties are constructed by language and connected to a specific discourse and ideology. In the case of the British newspapers' framing of the Deep Web, negative uses are interspersed, normalised and even derided in the coverage. In some cases, these technologies are addressed with disbelief. *The Guardian*[63] published an article in November 2016 about retail services on the Dark Web, pointing out that:

```
The academics say the sites, once accessed by invitation or via dark-web
(there'll be no hyperlinks here) resemble typical marketplaces such as Amazon
or eBay.
```

Although the Web has reached a stage of maturity in most developed countries, it continues to feed the imaginary of people while dealing with dreams and imagination (Malbreil, 2007). In the case of the Deep Web, as Gehl (2016) suggested, this empirical research demonstrates that the press persistently adds to this imaginary a negative dimension of darkness and illegality. This chapter reveals that this representation by the British press is made in such a way that the Deep Web is considered negative, inexplicable and opaque. It is negative because the concepts related to the Deep Web are composed of metaphors, so the choice to persist with an undesirable metaphor such as the Dark Web is related to harmful uses and associations. It is also inexplicable because there is a general lack of effort in providing comprehensive definitions and explanations about these technologies, with an almost complete omission of specialised sources, showing limited interest in acutely explaining these systems. And it is opaque because language and attributes are used to add a layer of murkiness to these technologies.

[63] Related article: "Dark Web departure: fake train tickets go on sale alongside AK-47s," The Guardian, 2nd November 2016, Technology, page 3.

5 "This is the Wild West": The Deep Web and Hyper-Panic

Addressing criminal uses of the Deep Web, especially the operation of the crypto market Silk Road, a newspaper article[64] published by *The Times* in 2012 provides the following definition of the Dark Web: '[A] hidden part of the internet, where users are anonymous and can act without the apparent risk of being snooped upon by law enforcement. This is the Wild West, before the sheriffs came to town.' The comparison to the Wild West – the myth based in North American history and perpetrated by popular culture as a place ruled by criminals and where the law is continuously ignored – illustrates how British newspapers' discourse links these technologies to antisocial and criminal behaviours. This example and others discussed in this chapter show how media panic, typified as 'emotionally charged reactions on the appearance of new media' (Drotner, 1999, p. 593), surround the Deep Web.

This research shows that the British press not only portray the Deep Web as a threat, but they also constantly associate these technologies with several other social fears. This chapter argues that news media coverage of the Deep Web presents two types of panic condensed into one. The first panic is related to the Deep Web as a new medium, focusing on its affordances, opacity and purposes. The second panic is related to the potential uses of the Deep Web and how it can facilitate criminal activities that are per se social fears, such as the drugs trade, terrorism and paedophilia. Hence, this research suggests that the panic surrounding the Deep Web not only focuses on the technology, but also multiplies and increases other well-known forms of panic. This chapter draws on the content analysis results to discuss these multiple panic types associated with Deep Web technologies. The objective is to define the elements through which the media represent these technologies as a threat, and to interrogate to what extent other social fears appear in the coverage, by considering focus, context, sources and users.

Thus, the next section offers a definition of hyper-panic, conceptualised as a phenomenon in which media panic and moral panic are combined. In this case, a new medium, i.e. the Deep Web, is represented mainly in terms of enabling and facilitating social fears, such as child abuse,

[64] Related article: "Drugs, guns and passports for sale on 'Dark Web,'" The Times, 3rd April 2012, News, page 12.

terrorism and the trade of drugs. This section is followed by a discussion focused on the aspects that construct media panic related to the Deep Web. This chapter also addresses social fears raised by the British press about the Deep Web through an association with criminal and antisocial behaviours, common activities mentioned in headlines, rhetoric and terminologies applied to represent users and sources and their views. Finally, this chapter proposes a discussion not only on this new concept of hyper-panic, but also about position of the Deep Web's representation in the context of how the Web is usually portrayed.

5.1 Defining Hyper-Panic

Moral panic is a fear-producing process understood as the strong disapproval of moral threat (Garland, 2008) and established through a combination of media framing, right-thinking people and questionable experts nourishing this anxiety (Cohen, 2011). It is also defined by Hickman (1982, p. 9) as a phenomenon instigated by news media to play with the fear of crime and inflame a reaction 'completely out of proportion to the actual threat.' Paradoxically, the notion of threat created through the media can be more dangerous to a society than the crime, since it induces authorities' dialogue and actions for crime control in the direction of social fears and anxieties instead of in the direction of what statistics prove to occur (Hickman, 1982).

The emergence of the concept of media panic, a derivative of moral panic focusing on the rise of new media, occurred in the 1990s. This concept is related to the way new media are perceived shortly after they are introduced, considering that novelties promote transformations in society through the dichotomy of positive and negative views, which in turn encourages a public debate about social and cultural norms (Drotner, 1999). Comparing the concepts of moral and media panic, there is no clear distinction in the way fear is constructed and maintained, besides the fact that the underlying aspect in the second case is related to the emergence of new media.

Taking as an example computers and the discussion about their potential uses, Drotner (1999, p. 596) argues that there was polarisation between optimist and pessimists' views of that technology, a common reaction to novelties: '[T]he computer discourse is a complex constellation of pros and cons which together condense two fundamental discursive approaches

that have surfaced whenever new media have come to the fore in the past.' Computers are one of many examples over the course of history in which new media have divided social opinions. Video games, for instance, can offer positive outcomes such as cognitive thinking, skills development and ethical discussions, but they are commonly associated with the promotion of violence and alienation (Martin, 2012). In fact, games represent 'a variety of social anxieties: about youth violence, new computer technology, and the apparent decline in the ability of adults to control what young people do and know' (Sternheimer, 2007, p. 13), and these fears are broadly exploited in news coverage. Video games have been blamed, for instance, when episodes of violence have gamers as protagonists, such as mass shootings in schools in the United States of America, which many consider an idle approach by the news media, as they arguably neglect the authentic reasons why young people become violent in the first place (Sternheimer, 2007; Martin, 2012).

Another example of media panic is the controversy raised by the popularisation of mobile phones among youths, spreading a fear of activities that are not broadly understood by society such as sexting – defined as the practice of sending sexual content through text messages –, crime and cyberbullying (Hasinoff, 2012). Although mobile phones can indeed be used for sexting and other antisocial or criminal activities, this technology's purpose is encouraging communications and socialisation (Lim, 2013), with positive uses, for example educational research and a resource in the case of emergencies.

Also, specific smartphone applications have been the subject of media panic. Although a good number of successful relationships started this way, Tinder and other dating apps have a sharply negative portrayal related to promiscuous sexual behaviour, harassment, misogyny and other forms of contemporary sexism (Thompson, 2018). In another example, the instant messaging apps Telegram and WhatsApp became controversial for being used to spread fake news during political campaigns and elections (Iosifidis & Andrews, 2019) or to plan terrorist attacks (Magdy, 2016). Similar to Tor, which protects the user's privacy and avoids surveillance, these messaging apps have end-to-end encryption to safeguard communications, which makes it almost impossible to intercept chat content without having access to the device (Santos & Faure, 2018).

Even newspapers were themselves a reason for moral panic in the past. Furedi (2016) states that British elites reacted in a severely negative way to the spread of the press in the United Kingdom in the late 18th century, a response to the anxiety of reviewing societal norms and values, due to having a more critical working class. In a time in which the habit of reading was not as widespread as it is nowadays, the idea of a popular mass regularly gaining access to newspapers motivated fear of the media's effects: '[T]he intoxicating emotional, non-rational and even irrational passions that could be incited through the consumption of the media were perceived as a threat to rational order' (Furedi, 2016, p. 533).

It is ironic, to say the least, that nowadays the press is an instrument in the fear-producing logic. In fact, if the media can be the subject of panic, they can also promote panic being partially responsible when 'a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests' (Cohen, 2011, p. 1). As McRobbie & Thornton (1995) argue, both tabloid and quality newspapers in the United Kingdom contribute to moral panic by using an emotional discourse to grab the interest of readers and misrepresenting attitudes and activities. Besides that, 'moral panics have become the way in which daily events are brought to the attention of the public. They are a standard response, a familiar, sometimes weary, even ridiculous rhetoric rather than an exceptional emergency intervention. Used by politicians to orchestrate consent, by business to promote sales in certain niche markets, and by media to make home and social affairs newsworthy, moral panics are constructed on a daily basis' (McRobbie & Thornton, 1995, p. 560).

Media representation of the Deep Web, as this research discusses, embraces anxieties similar to those raised by novelties such as computers (Drotner, 1999), video games (Sternheimer, 2007; Martin, 2012), mobile phones (Hasinoff, 2012; Lim, 2013) and newspapers (Furedi, 2016). Additionally, this research shows and has conducted content analysis demonstrating that newspapers in their coverage of the Deep Web also reinforce existent and well-known forms of panic in their day-to-day coverage. Therefore, this work proposes a new concept which embraces the idea of a core facilitator of antisocial and criminal behaviours and is responsible for amassing anxieties, i.e. a phenomenon in which primary media panic allows several types of secondary moral panic, as the next sections of this chapter show.

5.2 Primary Media Panic: The Dark Web

Discussing the relationship between new technologies and the construction of social meaning, Sturken et al. (2004) contend that emerging objects instigate a combination of fascination and concern related to their impact on society. Thus, new technologies can be perceived at the same time with optimism and hope, as well as with fear and anxiety. Nevertheless, according to Sturken et al. (2004, p. 1), pessimist visions are commonly related to the fact that 'technologies in their emergent stages have played a dramatic role in visions of the future and beliefs in the possibility of change.' Indeed, this research claims that the British press represent the Deep Web as an extra layer of sophistication to existent crimes, as well as a space for the development of new ones. This negative portrayal of the Deep Web is perceived when the media present affordances as threats, emphasise its technical opacity and undermine its purposes.

The concept of social affordances has its origins in the theory developed by Gibson (1979) and in general relates to the possibilities that a certain environment affords. Thinking of the example of animal life in a forest, for instance, the forest's affordances are bad and good weather, numbers of predators, food availability, shelter and other environmental circumstances provided by the forest that require the animal to adjust to survive. Adapting the term to interface design, Norman (2002) explains that affordances are related to the clues that an object provides about potential uses that can and cannot be achieved, thus limiting possibilities. In the case of new technologies, social affordances are related to specific uses which can emerge when personal knowledge and experience meet the clues provided by software or an application, potentially shaping this technology in new ways (Hsieh, 2012).

Analysing the Deep Web's representation by the British press, two main affordances are broadly portrayed as threats by newspapers, and the first one is providing online anonymity. In fact, the data show that discussions about online anonymity in the British press are typically related to the fear of how criminals can potentially use it. Articles can portray anonymity as something evil and unnecessary, as the example of "Beware turning drug dealers into folk

heroes"[65], published by *The Times*, discussing the claim that Silk Road developers are standing up for online freedom. This example shows how the fear of the unknown plays with the idea of online anonymity and minimises positive uses. In fact, in this article, the argument against online anonymity relies on the idea that:

```
What those who follow pirate politics often seem to forget is that empowering
the individual empowers nasty individuals too. Indeed, it probably empowers
them more. Strike a blow for digital liberties and the first to cheer are the
child pornographers. Then come money launderers, tax evaders, fraudsters,
terrorists and God knows who else.
```

The second affordance of Deep Web technologies constantly discussed by newspapers is protection against surveillance, which incites fears related to losing control of what happens online. In this sense, the British press constantly validate vigilant actions, as exemplified in the article "Large rise in internet users who mask their identity,"[66] also published by *The Times*, stating that:

```
Sir Tim Berners-Lee, the British inventor of the web, defended the right of
agencies to spy on web users. 'Sometimes people do have to spy on the internet
for law enforcement,' he said. 'We have to figure out how to balance that
against rights.
```

The same is seen in the article "SAS and MI5 hunt for cyber spy team,"[67] which celebrates the fact that two governmental agencies will invest together in cybersecurity. The article includes:

```
A unit will specialise in cyber warfare, including 'phishing attacks' which
steal data from terror networks, operating against propaganda platforms and
cloning sites on the 'dark web.' A senior military source said: 'Digital
surveillance and phishing missions are a key aspect of modern operations.
```

[65] Related article: "Beware turning drug dealers into folk heroes," The Times, 8th October 2013, Editorial/Opinion, page 25.
[66] Related article: "Large rise in internet users who mask their identity, The Times, 19th May 2014, News, page 16.
[67] Related article: "SAS and MI5 hunt for cyber spy team," The Sun, 7th August 2016, News, page 33.

Another aspect through which media panic is constructed in the case of the Deep Web is the use of the perceived opacity of these technologies, as mentioned in Chapter 4 (*Struggles of Meaning and Concepts: A Deep or Dark Web?*). Considering that this opacity is related not only to attributing a layer of secrecy to the technology, but also stressing the general lack of knowledge about how it works and/or can be used (Burrell, 2016), the British press overall illustrate the Deep Web as something mysterious, and they make little effort to provide deeper explanations. This is seen in the article "Class A… By 1st class,"[68] published by *Daily Mirror*, in which the description of how to access Silk Road is generic and limited, without a direct mention of the Tor Network or encryption, and with a superficial explanation of Bitcoin:

> Locating the site involved the use of a special downloaded web browser popular with criminals. It works just like Internet Explorer or Safari but hides the user's location. After registering on Silk Road - a pro-cess that only asks for you to choose a username and password - an astonishing illegal drugs market place opened up. As well as cocaine, ketamine, MDMA - the main component of ecstasy tablets - and types of cannabis, there were also steroids, morphine-like opioids, psychedelics and a host of other illegal stimulants. The website also has sections for users who want illegal weapons, forged documents and porn. Unlike mainstream markets such as eBay and Amazon, transactions on Silk Road are made using the controversial internet-only currency Bitcoins. These can be bought online through an ordinary bank account and traded across the web between individuals with little chance of the cash source ever being traced.

Finally, the British press constantly publish articles questioning the purposes of the Deep Web, even the fact that it is actually available in the first place, consistently ignoring positive results. An example of how the existence of these technologies is treated by the media as something to fear is seen in "Parly dark web bids,"[69] published by *The Sun*:

> Computers in the Commons and Lords were used 250 times in the last year to try

[68] Related article: Class A… By 1st class," Daily Mirror, 25th May 2014, News, page 24.
[69] Related article: "Parly dark web bids," The Sun, 17th October 2015, News, page 4.

```
to access the ‘dark web,’ The Sun can reveal. The hidden network is notorious
for sites selling drugs, guns and child porn. Security checks would have
blocked the attempts, officials said. Users were attempting to download Tor
software, the most popular way in which to gain access.
```

In this instance, people that were trying to download a legitimate browser that can be used for many reasonable motivations were immediately connected to negative intentions related to drugs, paedophilia and other social fears. The next section of this chapter demonstrates how this connection is not an exception but the norm in British newspapers’ coverage.

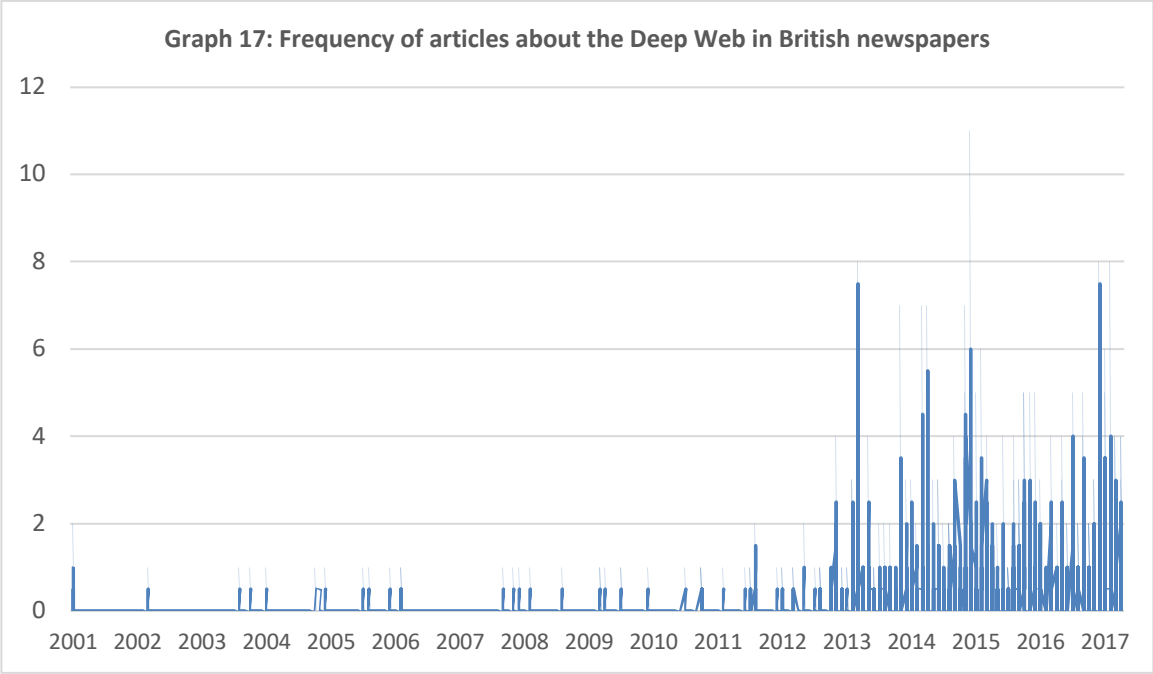
5.3 Secondary Moral Panic: Drugs, Paedophilia, Terrorism and More

Considering that the phenomenon defined in the previous section as hyper-panic is composed of a primary media panic allowing several other forms of moral panic, the aim of this section is to discuss to what extent these secondary social fears appear in British newspapers’ coverage of the Deep Web. In addition, this research demonstrates in the next sections that the association between the Deep Web and criminal and antisocial behaviours is made via four main avenues: episodic coverage focusing on negative uses, the normalisation of illegal or immoral activities in headlines, sharply condemning rhetoric used to describe users and the favouritism of official sources with conservative views.

The rhetorical construction of media panic through newspaper coverage is seen not only in the discourse used to describe the new medium, but also in topics associated with it. As this empirical research shows, the Deep Web is continuously portrayed as a threat to society, which can be seen through the topics the media consider newsworthy (Cohen, 2011). This section identifies those topics emphasised by British newspapers when selecting extraordinary episodes related to the Deep Web. The commonest theme is crime. As Garland points out (2008, p. 18), this logic is engaged and expected by the audiences, due to the ‘excitement and energy that are unleashed by moral panic episodes, as well as the enjoyment generated by these collective waves of righteous condemnation.’

Episodic coverage is a media approach typified by punctual increases in the amount of publications about a topic during specific events associated with the use of personal

understandings and experiences of present issues, instead of a broader examination of the general context in an analytical manner (Iyengar, 1990). Vasterman (2005) uses the expression 'media-hype' to define these moments in which 'every now and then, the daily news media suddenly generate surprisingly high news waves on one specific story.' This can be seen in the British press coverage of the Deep Web (Graph 17), since looking at the frequency of articles published by the researched newspapers over time, there is regularity in the number of articles with atypical moments in which the volume sees a significant rise.



This research identified six events in which there was greater attention paid to the Deep Web, as it happened in episodic coverage (Iyengar, 1990; Vasterman, 2005). Three conditions were considered when selecting these cases (Table 11). First, the articles mentioned "Deep Web" or any other variation of the term previously cited (see *Methodological Framework*), second, the topic counted at least one publication by each of the six researched newspapers, proving that it was addressed by every quality and every tabloid included in this analysis, and third, at least half of the newspapers had more than one published article about the topic over a period of two weeks, showing that the interest was not singular or isolated.

Table 11: Episodic coverage and number of publications by newspaper

MAIN EVENTS IN THE COVERAGE	NUMBER OF ARTICLES						TOTAL
	Daily Mail	Daily Mirror	The Sun	Daily Telegraph	The Guardian	The Times	
Event 1	1	1	2	4	2	4	14
Event 2	1	2	2	2	1	3	11
Event 3	1	3	3	2	2	3	14
Event 4	1	3	4	6	3	2	19
Event 5	9	2	2	1	1	1	16
Event 6	8	11	6	5	2	1	33

These six events are listed in chronological order and briefly summarised as follows, according to the information provided by the researched newspapers.

Event 1: Silk Road's Closure (October 2013)

Available through Tor Hidden Services since 2011, Silk Road was the most famous and active crypto market on the Deep Web. Widely used in the trade of drugs, Silk Road mainly connected sellers to smaller sellers and users, and scholars have proposed to consider it as a transformative tool for potentially reducing face-to-face interactions in this market – and therefore violence (Aldridge & Décary-Hétu, 2014). The closure of Silk Road by the FBI in October 2013 was the first event related to these technologies being broadly covered by the media, and it was only possible because of the arrest of Ross Ulbricht, supposedly the founder and developer of the website, in San Francisco, United States of America. Newspaper coverage had a total of 14 articles – four published by tabloids and 10 by quality newspapers – focusing not only on explaining how crypto markets work, but also on the figure of Ulbricht, represented as the "mastermind" behind the e-commerce operation.

The Daily Telegraph, for instance, published four articles about the subject, one of which was an editorial entitled "You'll soon be able to buy that AK47 again; The FBI has closed one secret

online market, but another is bound to open before long,"[70] which explains why Silk Road's closure unveiled the extension of the online trade of drugs. The article includes the sarcastic sentence:

```
I am sorry if it offends any readers who recently made an order on the 'dark
internet' site, which supplied every drug known to humanity and a range of
other illegalities, but there is no sugaring this particular pill. Face it,
suckers, the crystal meth ain't coming in the post.
```

This emotional and judgmental discourse, including how the author refers to users, indicates the attribution of panic (Hickman, 1982; Garland, 2008; Cohen, 2011). It also summarises the way the newspapers portray this crypto market, i.e. the overall picture of Silk Road in this context is an immoral website used for harmful purposes.

Event 2: Prime Minister's Speech (December 2014)

In December 2014, the then Prime Minister David Cameron announced during a speech at an online global summit in London a new specialist unit that would focus on fighting child abuse. Bringing together the Government Communications Headquarters (GCHQ) and the National Crime Agency (NCA), the new unit was dedicated to identifying not only abusers, but also people distributing child pornography material over the Internet – the reason why the Dark Web was widely mentioned in the coverage. In the same speech, Cameron thanked technology companies that block this kind of material and help authorities to identify suspects, and he also mentioned that the same technology can assist investigations against terrorist groups.

There are 11 articles in total about this topic, five in the tabloids and six in quality newspapers, and the coverage of *The Times* accounts for three. One article entitled "Spy agency prowls dark net to snare worst child sex offenders"[71] includes part of Cameron's speech, saying:

[70] Related article: "You'll soon be able to buy that AK47 again," The Daily Telegraph, 5th October 2013, Editorial, page 25.
[71] Related article: "Spy agency prowls dark net to snare worst child sex offenders," The Times, 11th December 2014, News, page 15.

> Every time someone chooses to view an online image or a video of a child being abused, they are choosing to participate in a horrific crime. Every single view represents that victim being abused again. They may as well be in the room with them. The so-called 'dark net' is increasingly used by paedophiles to view sickening images. I want them to hear loud and clear, we are shining a light on the web's darkest corners; if you are thinking of offending there will be nowhere for you to hide.

In this representational example, the official discourse demonstrates a very negative overview of these technologies, through terms such as "horrific crime," "sickening images" and "darkest corners." Besides the emotional aspect, the British authority openly establishes the Dark Web as a public threat (Hickman, 1982) and spreads fear, assuring that it is a target for investigations, seen especially in the expression "we are shining a light."

Event 3: Ricin and the Crypto Market (July 2015)

In July 2015, the media broadly covered the trial of a British man who ordered 500g of a poison called ricin from the Dark Web crypto market Evolution Marketplace, an amount sufficient to kill more than a thousand people. In this case, newspapers compared the man to the main character of the TV series *Breaking Bad*, since ricin was the chemical used by the personage to kill enemies without leaving a trace. This case also involved an undercover FBI agent who was in touch with the suspect and negotiated the poison's sale, and it was considered a terrorism act, because the amount of ricin was equivalent to a chemical weapon with the potential for mass murder.

With 14 articles in total, half published by tabloids and half by quality newspapers, this case resulted in the following headlines on 22nd July 2015, the day after the trail started:

Daily Mail	Terror suspect called Weirdo ordered enough ricin to kill 1,400
Daily Mirror	Dad ordered enough ricin to massacre 1,400
Daily Telegraph	Tech worker caught buying ricin on the web
The Guardian	Man ordered 'Breaking Bad-style' ricin delivery from FBI agent, court hears
The Sun	'What poison kills quick and is hard to detect'; ricin geek search on net

The Times | Man 'paid for enough ricin to kill 1,400'

These headlines show a strong and condemnatory discourse, which is evident by the mention to the amount of people that could have been harmed by the chemical in half of the headlines, by the reference to the poison in all examples and, in a severe instance, by the use of the word "massacre" in the *Daily Mirror* headline.

Event 4: Ashley Madison's Data (August 2015)

One event caused special commotion in the media in August 2015, when a hacker group called Impact Team published sensitive and confidential details of 33 million users of the Canadian website Ashley Madison on a Deep Web forum. What made this data leaking intriguing is the fact this it is a dating website focused on facilitating extramarital affairs. In fact, this objective is openly identified on the website: '[E]very day, thousands of people join Ashley Madison to find discreet relationships of all kinds. Single, attached, looking to explore, or just curious to discover what's out there – Ashley Madison is the most open-minded dating community in the world.'[72] Data from 1.2 million British users, supposedly including a number of high-profile people, were leaked.

In total, 19 articles were published on the subject – 11 of them by quality newspapers and eight by tabloids. The coverage by *The Daily Telegraph* included six articles, with the following headlines, in order of publication: "Revealing too much"[73]; "Scientists and MP named on adultery website"[74]; "Ashley Madison founder's emails leaked in latest data dump"[75]; "Exposed: so what happens next?"[76]; "Adultery site's 'King of Infidelity' quits after scandal"[77] and "Spy agencies

[72] Available on https://www.ashleymadison.com/ Access: January 2019.
[73] Related article: "Revealing too much," The Daily Telegraph, 20th August 2015, Editorial, page 19.
[74] Related article: "Scientists and MP named on adultery website," The Daily Telegraph, 20th August 2015, News, page 1.
[75] Related article: "Ashley Madison founder's emails leaked in latest data dump," The Daily Telegraph, 21st August 2015, News, page 15.
[76] Related article: "Exposed: so what happens next?," The Daily Telegraph, 22nd August 2015, News, page 26.
[77] Related article: "Adultery site's 'King of Infidelity' quits after scandal," The Daily Telegraph, 29th August 2015, News, page 10.

mining adultery website data"[78]. This set of articles shows that *The Daily Telegraph* coverage initially concentrated on the leaked data, by naming users, although the articles ironically mentioned the lack of ethics of the hackers for making the information public, then its attention turned to the company that owns the website, with news about the founder, and, finally, it looked at the practical outcome of the situation, i.e. the information being used to blackmail Ashley Madison's users.

Event 5: Cyber-Attack on TalkTalk (October 2015)

One of the most prominent cyber-attacks in the history of the United Kingdom was made public in October 2015 and referred to the case of the telecom company TalkTalk. In this attack, hackers gained access to entire database holding the personal information of allegedly 4 million customers, including bank and credit card details, dates of birth, phone numbers and addresses among other data. These details were then offered in packages via crypto markets on the Dark Web to people interested in stealing someone's identity for purposes such as blackmail and fraud.

This coverage includes 16 articles by the six researched newspapers: 13 in tabloids and three in quality newspapers. *Daily Mail* is responsible for more than a half of this number, with nine articles on the subject. The first of them is entitled "The Dark Web"[79] and explains how this technology is connected to the cyber-attack:

```
A big concern is that this information could be put up for sale on the dark
web' – the expanse of internet space hidden to most users, but not gangs of
cyber criminals.
```

Other headlines from the same newspaper were directly alarming, such as "Victims of TalkTalk hack to be targeted,"[80] "Babyface hacker who paralysed a phone giant,"[81] "Auction

[78] Related article: "Spy agencies mining adultery website data," The Daily Telegraph, 31st August 2015, News, page 7.
[79] Related article: "The Dark Web," Daily Mail, 25th October 2015.
[80] Related article: "Victims of TalkTalk hack to be targeted," Daily Mail, 26th October 2015.
[81] Related article: "Babyface 'hacker who paralysed a phone giant,'" Daily Mail, 28th October 2015.

websites where criminals gangs trade your bank details for £23"[82] and "It's not just TalkTalk: hackers hit 14 new firms[…] and sell your details on 'Dark Web'"[83].

Event 6: Kidnap of Chloe Ayling (August 2017)

The latest event identified by this research is the kidnap of the British model Chloe Ayling, who was taken during what she thought that was a professional appointment in Italy in August 2017 and kept in captivity to be auctioned through the Dark Web and sold as a sex slave. In the end, she was released before the auction and returned to the United Kingdom in safety. Afterwards, Ayling was accused of staging her own kidnap to become famous. This is event had the most extensive coverage by British newspapers in the context of Deep Web technologies. In total, 33 articles were published about the case: 25 of them by tabloids and eight by quality newspapers. *Daily Mirror* leads the coverage, being responsible for 11 of the articles.

In chronological order, *Daily Mirror* published articles with the following headlines: "No safety net for the dark web,"[84] "Last thing she remembers is suitcase pulled over her head,"[85] "Evil of Dark Web,"[86] "Feared thugs trade sex slaves online,"[87] "I woke up bound & gagged with adhesive tape, inside a bag in a boot of a car…,"[88] "We built up a trusting relationship[…] He bought me shoes and fresh knickers,"[89] "Kidnap mum sets her eyes on stardom,"[90] "Kidnap of model: ransom demand for 3 men in UK,"[91] "Scourge of slavery must be exposed,"[92] "Police took control

[82] Related article: "Auction websites where criminals gangs trade your bank details for £23," Daily Mail, 28th October 2015.
[83] Related article: "It's not just TalkTalk: hackers hit 14 new firms… And sell your details on 'Dark Web,'" Daily Mail, 1st November 2015.
[84] Related article: "No safety net for the dark web," Daily Mirror, 6th August 2017, Features, Page 4.
[85] Related article: "Last thing she remembers is suitcase pulled over her head," Daily Mirror, 6th August 2017, News, page 4.
[86] Related article: "Evil of Dark Web," Daily Mirror, 6th August 2017, News, page 12.
[87] Related article: "Feared thugs trade sex slaves online," Daily Mirror, 7th August 2017, Features, page 16.
[88] Related article: "I woke up bound & gagged with adhesive tape, inside a bag in a boot of a car…," Daily Mirror, 7th August 2017, Sport, page 14.
[89] Related article: "We built up a trusting relationship… He bought me shoes and fresh knickers," Daily Mirror, 8th August 2017, News, page 4.
[90] Related article: "Kidnap mum sets her eyes on stardom," Daily Mirror, 9th August 2017, News, page 4.
[91] Related article: "Kidnap of model: ransom demand for 3 men in UK," Daily Mirror, 11th August 2017, News, page 24.
[92] Related article: "Scourge of slavery must be exposed," Daily Mirror, 13th August 2017, Features, page 28.

of computer to hunt down kidnap gang"[93] and "Cops hold brother of model kidnap suspect."[94] The use of the victim's sentences as headlines, which shows the personal experience aspect of the coverage (Iyengar, 1990) and the adoption of sharp language such as "evil," "scourge" and "sex slaves," exemplifies how such coverage can portray an isolated case as a social threat.

The Deep Web as a Multiplier of Existing Fears

Although each matter in episodic coverage can be presented in distinct ways by the media, and 'a reader with no prior knowledge of the events could get a very different perspective on the story depending on which newspaper they followed' (Branum & Charteris-Black, 2015, p. 216), overall these six occurrences allow for general assumptions about British newspapers' representation of the Deep Web. These episodes visibly connect these technologies to the event of a crime that is a moral panic. This can also be seen in the discussions about mobile phones and the fear of being used for criminal or antisocial purposes (Hasinoff, 2012; Lim, 2013).

The closure of Silk Road (Event 1), covered by 14 articles, is the trigger for regular coverage of Deep Web technologies, since the overall volume of articles was minor before October 2013. From that point, British newspapers consistently published content about crypto markets, explaining how they work and also going through technical aspects with information, for instance, about how anonymity is granted on the Tor Network and how crypto currencies such as Bitcoins are used in transactions. In addition, Silk Road is also a special case because it is mainly related to the commerce of drugs, a topic that receives greater attention from the British press, which commonly reproduce stereotypes, present superficial debates and contribute to the exclusion of drug addicts (Taylor, 2008).

Moreover, the topics connected to the Deep Web by the newspapers have in common the fact that they are all, individually, reasons for moral panic. Events 1 and 3, for instance, have stories focusing on crypto markets and the trade in drugs and chemical weapons, topics that

[93] Related article: "Police took control of computer to hunt down kidnap gang," Daily Mirror, 13th August 2017, News, page 12.
[94] Related article: "Cops hold brother of model kidnap suspect," Daily Mirror, 17th August 2017, News, page 25.

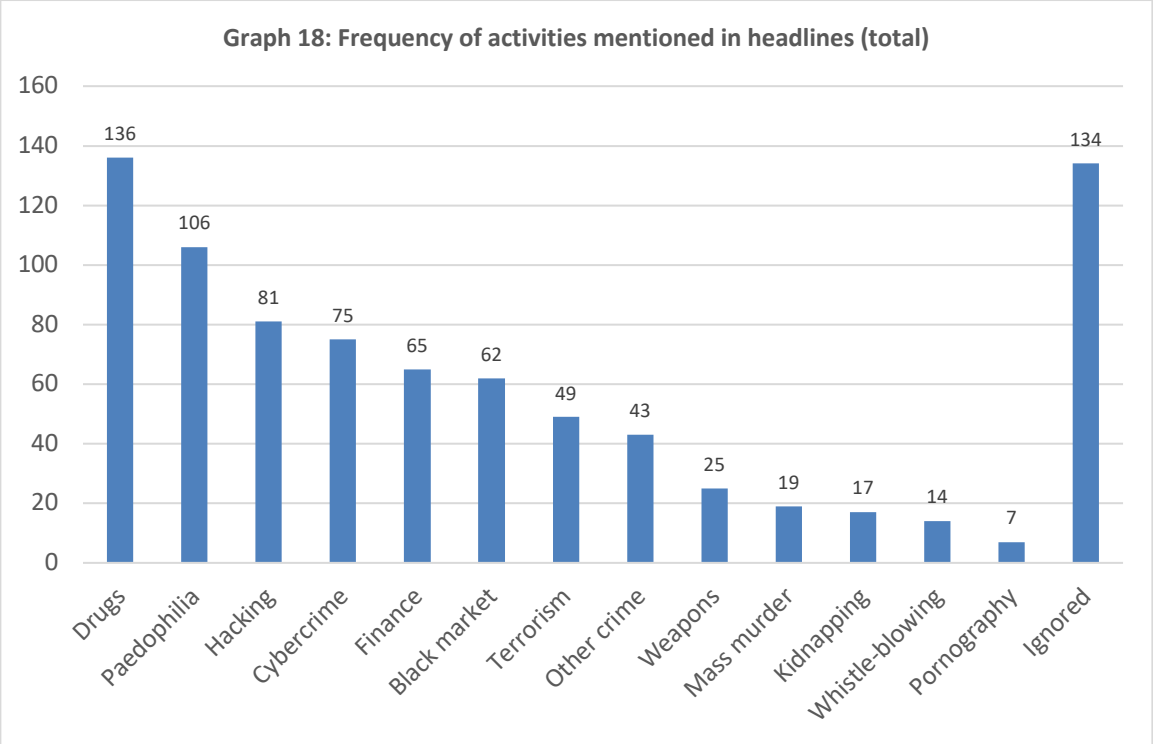
enjoy the consistent attention of the British press. Indeed, the widespread moral panic regarding drugs constantly plays with the fear of the social impacts of addiction (Taylor, 2008). In the case of Event 2, about a governmental investigation into the online distribution of paedophilia material and terrorist organisations, two topics that are constantly addressed by the British press in a moral panic rhetoric are brought together (Campbell, 2016; Ahmed & Matthes, 2017). The emphasis on authorities' efforts to fight crime and give an official response to the threat is part of the fear-producing logic (Cohen, 2011).

Related to both episodes with the highest numbers of publications – Event 6 involves coverage of the kidnap of the model Chloe Ayling, with 33 articles, while Event 4 spotlights the Ashley Madison data-leaking incident, with 19 articles –, they both have in common the exasperating layer of moral panic surrounding sex. The British press usually emphasise cases violent and sexual in nature in their daily coverage, which can direct the public attention towards these crimes and especially to the way that the justice system responds to them, once more contributing another level of panic (Surette, 1992). Furthermore, sexual crimes are over-represented by British newspapers, with both tabloid and quality publications adopting a negative, heated and emotional discourse on the subject (Harper & Hogue, 2014).

Finally, these six events are a sample of the media's daily coverage of the Deep Web and, as this analysis shows, the Deep Web is seen as platform on which distinct crimes are committed. Considering that each episode plays with one or more established societal fears, the overall representation of the Deep Web is interspersed with panic. Drugs, paedophilia, terrorism, hacking and other crimes are already a recurrent part of British newspapers' coverage, independent of the Deep Web. In this episodic coverage, though, the Deep Web adds a layer of fear to each case, because it is seen as a technological resource that facilitates crime and is thus a threat to the authorities fighting crime. In a sense, the representation of the Deep Web is not only about the technology but its position as a multiplier of existing fears and panic. This research argues that this phenomenon called hyper-panic can be identified also through the commonest topics in the headlines of articles, as showed in the next item.

5.4 Fear and Threat in Headlines

More than a summary of the topic, headlines provide an overall picture of the news article's content and are responsible for capturing readers' attention, influencing opinions (Reah, 2002) and proposing a specific understanding and interpretation of an issue (Bignell, 2002). Thus, they are responsible for setting the tone of the article. Considering this notion, and also that fear is constructed through rhetoric with a sharp, negative and condemning discourse (Cohen, 2011), this research examines headlines to trace the links made between the Deep Web and its uses. The examination of issues addressed in headlines shows compellingly that in 82.2% of the cases British newspapers associate these technologies with criminal or antisocial behaviours (Graph 18).

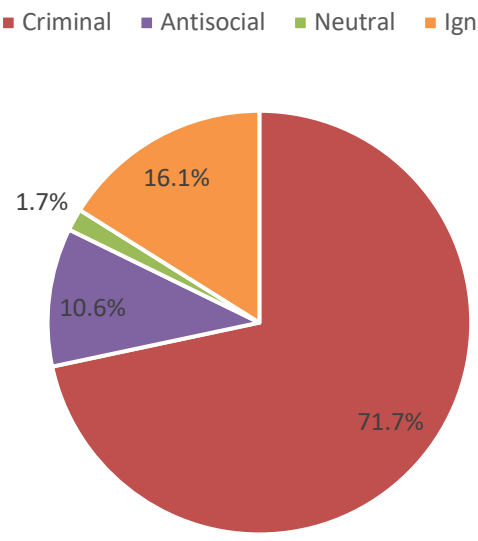


Looking at the central topic of the articles is fundamental to understanding the construction of knowledge through media, since representation reproduces political discourses (Orgad, 2012), and analysing media content unveils meaning (Bignell, 2002). As Graph 18 shows, this research identified 13 recurring topics addressed in the headlines. The criterium for this selection was that

the topic had at least six publications, which means an average of one by each analysed newspaper. Within these topics, 10 of them are directly related to crime (drugs, paedophilia, cybercrime, black market, terrorism, other crime, weapons, mass murder, finance and kidnapping), two of them are considered antisocial behaviour in the context of the British press (hacking and pornography) and only one of them is neutral, namely whistle-blowing. These 13 topics were directly mentioned in 699 headlines out of a total of 833 articles, which means 83.9% of the cases.

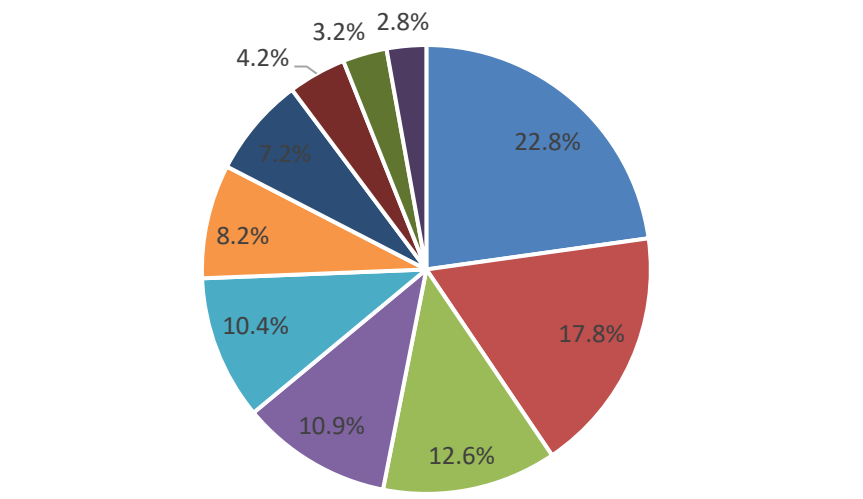
In the British context, coverage of crime by the media is directly related to fear of the same crime, since most people experience criminality only while reading or watching the news, which means that society is mostly subjected to a representation of the crime and does not face the criminality itself (Chadee & Ditton, 2005). Knowing that the media occupy a relevant role in the representation of crime 'shaping community identity and personal and shared senses of fear and (in)security' (Banks, 2005, p. 169), it is expected that readers of British newspapers see the Deep Web as a threat. Through a sharply negative rhetoric, the media consistently associate these technologies with misbehaviour, emphasising illegal uses in 71.7% of the cases (see Graph 19) and raising a direct association between these systems and misconduct.

Graph 19: Nature of activities mentioned in headlines

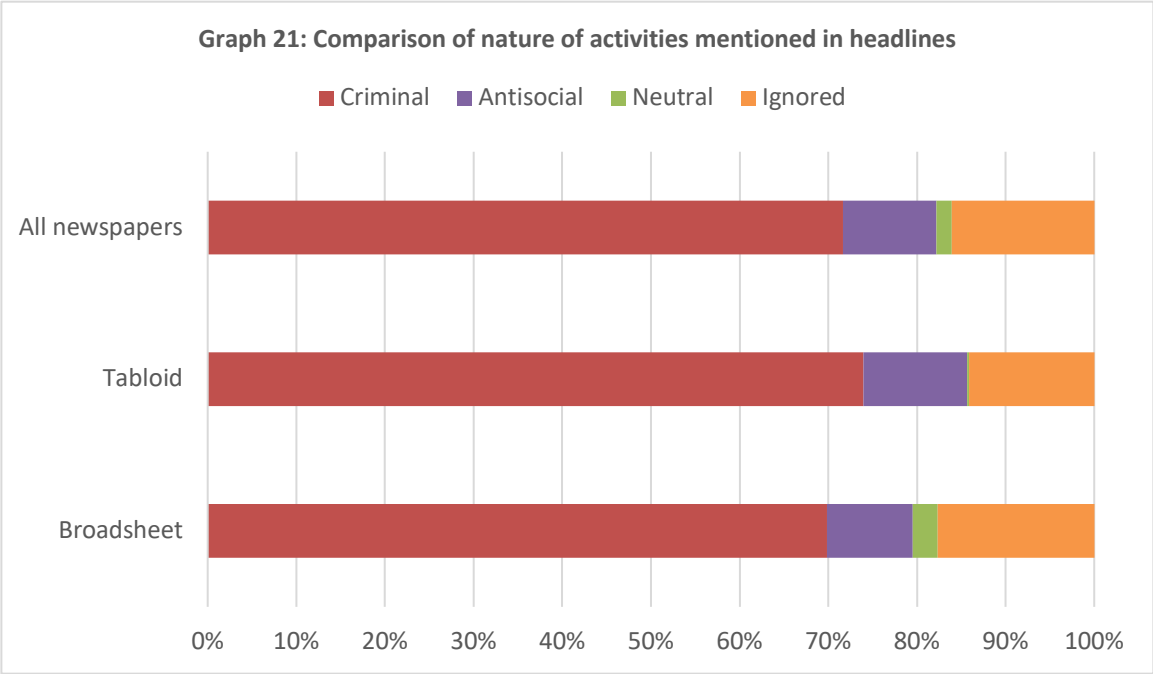


In terms of criminal activities addressed by the news (Graph 20), it is possible to see topics on which British newspapers focus their attention. The most recurrent topic associated with these technologies, for instance, is drugs, making up 22.8% of the cases and including headlines mentioning specifically some kind of drug, poison, toxin, overdose, medicine addiction, death caused by drugs, legal highs or drugs market available on the Deep Web. This is not a surprise, since British newspapers are responsible for the extensive coverage of issues related to drugs, albeit with an overall superficial discussion about the topic (Taylor, 2008). The second crime among the higher number of headlines is paedophilia, with 17.8%. The distribution of child pornography is a crime that not only holds the major attention of the British press, but also instigates digital vigilantism (Campbell, 2016). Cybercrime is also a recurrent topic in the media, with 12.6% of the headlines mentioning cyber or digital attacks or threats, victims of leaking of personal (such as celebrity photo) or corporate information, identity theft, online scams and/or computer viruses. The frequency of other topics can be seen in Graph 20.

Graph 20: Criminal activities mentioned in headlines



There is a subtle distinction between the representations of the quality and tabloid newspapers in terms of connecting these technologies to crime (Graph 21), with more emphasis in the case of tabloids, as expected, since they are generally more incisive when reporting on violence (Skovsgaard, 2014). In fact, articles addressing crimes represent 73.9% of the total for tabloids, against 69.9% for the quality newspapers. Publications that highlight antisocial behaviour represent 11.7% of tabloid articles, and 9.7% of quality publications. According to the Anti-social Behaviour, Crime and Policing Act 2014 (p. 2), published by the UK government, antisocial behaviour means, among other things, 'conduct that has caused, or is likely to cause, harassment, alarm or distress to any person,' which is why this category includes hacking and pornography, which are not crimes per se.



Another distinction is the fact that 2.8% of the quality articles have a neutral topic, while only 0.3% of the tabloids connect the Deep Web to a neutral activity in their headlines. This research considers whistle-blowing the only neutral activity. As Near & Miceli (1996) argue, there is an aspect of sensationalism in the way instances of whistle-blowing are treated by the media, especially because the whistle-blower is seen as someone eccentric and disloyal, simply for taking

action and reporting misconduct in a corporation or government. Although this role is part of the democratic system and 'a means to control illegal organizational behaviour' (Near & Miceli, 1996, p. 523), the activity of whistle-blowing is strongly controversial, and so it gains media's attention and is addressed from opposing perspectives according to the newspaper, which is why this research defines it as neutral.

In total, 14 articles were published by the six newspapers about whistle-blowing, with only one in a tabloid and the rest in quality newspapers. The tabloid's article is entitled "Snowden leaks made paedophiles harder to trace, says ex-MI5 chief,"[95] and was published by the *Daily Mail*. This headline was categorised herein as whistle-blowing instead of paedophilia, because the focus of the article is the content of the revelations, in that it paints a negative picture of whistle-blowing through a personal statement that suggests that paedophiles benefited from the activity. The discourse associating very distinct activities such as whistle-blowing and paedophilia exemplifies the way fear is constructed in the news.

An example of the same topic published in a quality newspaper is the headline "Edward Snowden's app to protect whistle-blowers from spies,"[96] which leads to *The Times*' article about Heaven, a counter-surveillance app released by the Freedom of the Press Foundation whose aim is to protect online communications. The article has a positive approach to the topic, discussing the relevance of the role of the whistle-blower and how the democratic right to report organisational crimes has to be protected. This example, compared to the previous one, also shows how newspapers can portray controversial issues from contrasting angles.

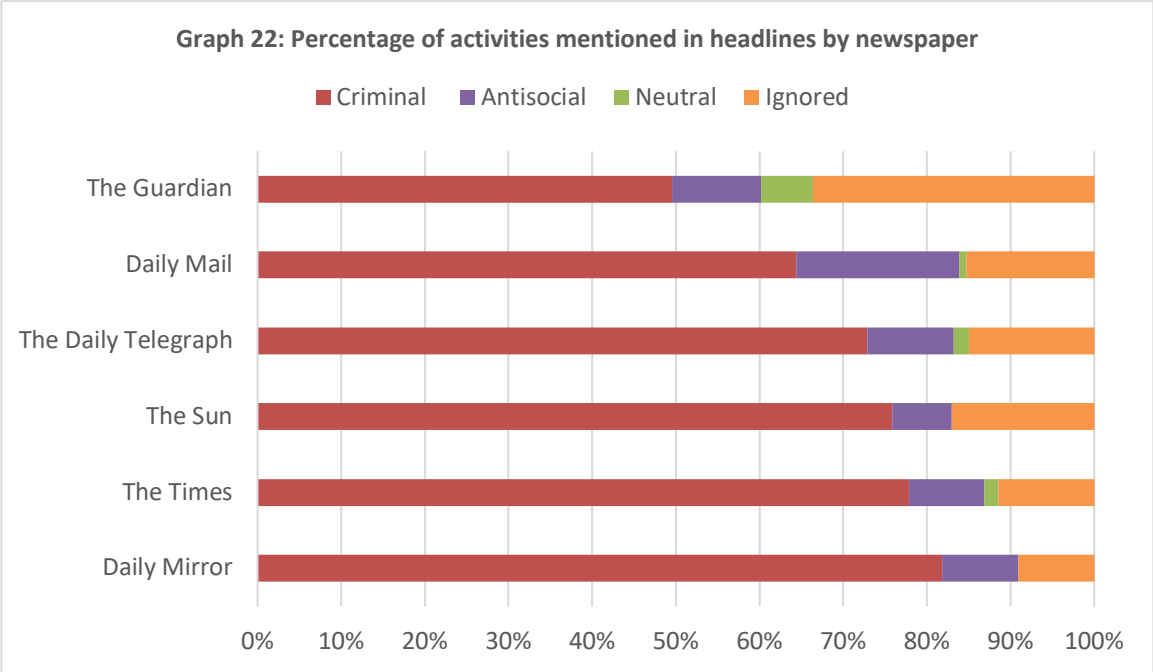
Finally, in 16.1% of the cases, none of these activities was cited in headlines, totalling 134 articles. Presented in the previous graphs as "ignored," these occurrences include articles that do not feature the above-mentioned activities. They comprise, for instance, headlines such as "In the land of the trolls,"[97] a review of Jamie Bartlett's book "The Dark Net" published by *The Times*;

[95] Related article: "Snowden leaks made paedophiles harder to trace, says ex-MI5 chief," Daily Mail, 12th August 2017.
[96] Related article: "Edward Snowden's app to protect whistle-blowers from spies," The Times, 28th December 2017, News, page 3.
[97] Related article: "In the land of the trolls," The Times, 23rd August 2014, Features, page 44.

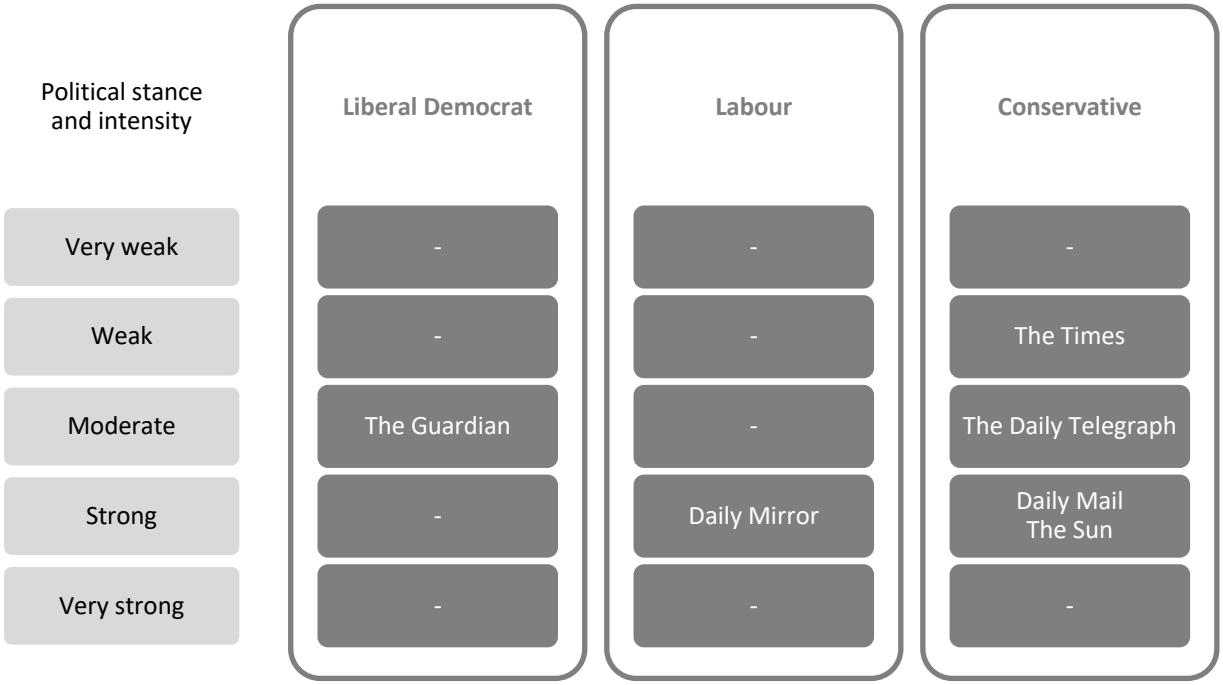
"DarkNet,"[98] an article in *The Sun* which presents an overview of how criminals can use these systems; "GCHQ spies bid to tackle Dark Web,"[99], a story in *Daily Mail* about British agencies tracking paedophilia; "The dark sci-fi that's reflecting modern life,"[100], published by *The Daily Telegraph* about a TV series with dystopic stories; "Heathrow security secrets are found lying in street,"[101] an article circulated in *Daily Mirror* about a memory stick found with information related to the airport and the risks of having these details unveiled on the Dark Web, and "We'd never kill an albatross or gorilla: but we let others do it on our behalf,"[102] an article in *The Guardian* about the trade in illegal ivory.

Looking at the newspapers separately (Graph 22) provides insights into the approach of each publication, considering that not only do different newspapers tend to stress distinct topics, but also that tabloids and quality newspapers' approaches are also guided by their political stance (Graph 23), as previously mentioned in the *Methodological Framework*.

[98] Related article: "DarkNet," The Sun, 19th April 2015, News, page 8.
[99] Related article: "GCHQ spies bid to tackle Dark Web," Daily Mail, 19th November 2013.
[100] Related article: "The dark sci-fi that's reflecting modern life," The Daily Telegraph, 27th December 2017, News, page 27.
[101] Related article: "Heathrow security secrets are found lying in street," Daily Mirror, 29th October 2017, News, page 4.
[102] Related article: "We'd never kill an albatross or gorilla: but we let others do in on our behalf," The Guardian, 14th September 2016, Opinion, page 33.


Graph 22: Percentage of activities mentioned in headlines by newspaper
Criminal
Antisocial
Neutral
Ignored
The Guardian
Daily Mail
The Daily Telegraph
The Sun
The Times
Daily Mirror
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Graph 23: Political stance and intensity of researched newspapers



Source: Wring & Deacon, 2010; YouGov, 2017

There are also important differences in the coverage of each newspaper (Graph 23), which may relate in significant ways to their political stance, as identified by Wring & Deacon (2010). Having a moderate Liberal Democrat approach, *The Guardian* is focuses least on the criminal uses of the Deep Web, although the number is still high, with 49.5% of its articles mentioning crimes in the headline, and 10.6% citing antisocial behaviours. In fact, this newspaper provides a range of examples of headlines for articles discussing the Deep Web, without a condemning discourse towards these technologies, such as "Libraries: the hidden potential of the web,"[103] "A thirst for knowledge,"[104] "Surveillance and the limits of GCHQs powers"[105] and "The irresponsibility of giant tech companies."[106] This demonstrates that *The Guardian* engages in opportunities to show

[103] Related article: "Libraries: the hidden potential of the web," The Guardian, 21st April 2004, Guardian ePublic, page 18.
[104] Related article: "A thirst for knowledge," The Guardian, 13th April 2006, Technology, page 1.
[105] Related article: "Surveillance and the limits of GCHQs powers," The Guardian, 24th June 2013, Leader Pages, page 27.
[106] Related article: "The irresponsibility of giant tech companies," The Guardian, 31st August 2016, Technology, page 32.

not only their positive outcomes, but also the sociological contexts and the surveillance logic in which these technologies are used.

Moreover, it is interesting to notice that although *Daily Mail* takes a strong conservative approach, this newspaper focuses less on criminal uses than the quality newspapers *The Daily Telegraph* (moderate conservative) and *The Times* (weak conservative). In the case of *Daily Mail*, 64.4% of the articles were related to crime and 19.5% to antisocial behaviour. This elevated number takes on a new perspective when compared to the approach of *Daily Mirror* (strong Labour), with 81.8% of headlines connecting the Deep Web to crimes and 9.1% to antisocial behaviours, the most negative coverage of the newspapers. In fact, *Daily Mirror* is responsible for the publication of headlines that relate these technologies to criminal uses through strong and emotionally charged language, such as "UK & US fight web paedos,"[107] "PM orders Google: do more to fight evil"[108] and "Web safety threatened by dark net."[109]

Finally, and still according to Graph 22, another point to highlight is that *The Times* is the quality paper with the most negative coverage of the Deep Web, with 77.8% of the headlines connecting it to crimes and 9.0% to antisocial behaviours, and the second among all the newspapers. Although *The Times* has a weak conservative discourse, this newspaper published a number of alarming headlines, such as "Military secrets for sale on dark web,"[110] "Terror police 'halted bid to buy ricin in dark web,'"[111] "Excluded teenager plotted a massacre"[112] and "New age of criminality leaves police struggling to catch gangs."[113] This shows that, although there are variations in the ways newspapers address the topic, negative uses of the Deep Web are seen not only in tabloid coverage: all the newspapers under examination herein contribute to some extent to shaping the discourse about the Deep Web as a moral panic.

---

[107] Related article: "UK & US fight web paedos," Daily Mirror, 18th November 2013, News, page 2.
[108] Related article: "PM orders Google: do more to fight evil," Daily Mirror, 12th December 2014, News, page 2.
[109] Related article: "Web safety threatened by dark net," Daily Mirror, 28th January 2015, News, page 8.
[110] Related article: "Military secrets for sale on dark web," The Times, 14th January 2015, News, page 15.
[111] Related article: "Terror police 'halted bid to buy ricin on dark web,'" The Times, 18th February 2015, News, page 5.
[112] Related article: "Excluded teenager plotted a massacre," The Times, 31st July 2015, News, page 4.
[113] Related article: "New age of criminality leaves police struggling to catch gangs," The Times, 24th March 2016, News, page 18.

5.5 "The Dark Web Devil" and Other Users

In October 2017, the story of a man being prosecuted for the first time in the United Kingdom because of material found on the Dark Web received significant media attention, with publications in all six researched newspapers. The case involved a 28-year-old man with a PhD from University of Cambridge who was using Internet forums to attract victims and access personal photos, videos and information. In some cases, he used these to blackmail them into sending more material or even committing crimes and distributing the content over the Dark Web. The wave of strong repudiation that met his acts can be exemplified in the words of an article entitled "The Dark Web Devil,"[114] by *Daily Mirror*:

> Sick Dr Matthew Falder, 28, targeted more than 50 victims on the dark web, including a 15-year-old girl who he conned into sending topless pictures then threatened to make them public unless she sent more. The pervert, whose online names were '666devil' and 'evilmind,' told another schoolgirl he would post naked snaps of her to every house on her parents' street unless she agreed to his vile demands.

Considering that newspaper articles' headlines often include strong language to attract readers' attention (Reah, 2002; Bignell, 2002), this case is particularly extreme in this regard. The use of emotional words such as "sick," "pervert" and "vile" in the description of the man conveys strong and explicit disapproval of Falder's actions. Furthermore, there are situations in which Deep Web users are framed openly as villains, providing the idea that using these technologies links directly to evil actions and endeavours. This is the case for the word "fiend," for instance, used in an article entitled "Net closing in Dark Web filth"[115] published by *The Sun*, which points to the reasons why police should invest money in investigating it:

> Highly encrypted corners of the web which 20,000 twisted fiends now use daily to view sordid material.

[114] Related article: "The Dark Web Devil," Daily Mirror, 17th October 2017, News, page 7.
[115] Related article: "Net closing in Dark Web filth," The Sun, 11th December 2014, News, page 2.

If British newspapers have little wish to show the positive uses of the Deep Web, it is not a surprise that its users are consistently stigmatised – as seen when looking at distinct attributes used to refer to them (see Table 12). The most used name, in fact, is "criminal," with 98 occurrences through the six analysed newspapers. Although newspapers widely use this term, sometimes as a synonym for "suspect," the interpretation of this concept and idea is not that simple. In fact, literature in criminology has stressed for centuries that 'no man can be judged a criminal until he be found guilty; nor can society take from him the public protection, until it have been proved that he has violated the conditions on which it was granted' (Beccaria, 1872, p. 33), which makes the media a constant threat to a fair penal system when over-reporting crimes, especially those involving violence and sex (Mason, 2006).

Table 12: Frequency of attributes associated with Deep Web users by newspaper

	NEWSPAPER						TOTAL
	DAILY MAIL	DAILY MIRROR	THE GUARDIAN	DAILY TELEGRAPH	THE SUN	THE TIMES	
Abuser	2	0	0	1	0	0	3
Activist	0	0	2	0	0	0	2
Addict	1	1	1	0	0	1	4
Al-Qaeda	0	0	0	1	0	1	2
Arab	0	0	0	0	1	0	1
Backer	0	0	0	0	1	0	1
Bomber	0	0	0	0	1	1	2
Buyer	1	1	1	1	1	2	7
Captor	0	0	0	3	0	0	3
Client	0	0	1	0	0	0	1
Community	0	0	1	0	0	0	1
Connoisseur	0	0	1	0	0	0	1

Conspirator	1	0	0	1	0	0	2
Consumer	0	0	1	0	0	1	2
Costumer	0	1	1	1	0	2	5
Criminal	23	11	9	6	15	34	98
Crook	3	5	0	0	2	0	10
Cryptographer	0	0	0	0	0	1	1
Cyber-villain	0	0	0	1	0	0	1
Dealer	6	9	2	6	10	16	49
Defendant	3	0	0	0	0	0	3
Drug supplier	0	1	0	1	0	1	3
Drug user	1	0	2	0	2	1	6
Exploiter	0	0	0	1	0	0	1
Extremist	0	0	1	1	1	0	3
Fanatic	0	0	0	1	0	0	1
Fiend	0	0	0	0	1	0	1
Fraudster	2	0	3	1	1	4	11
Gang	0	6	3	5	3	7	24
Geek	0	0	0	0	1	0	1
Government	0	0	1	0	0	0	1
Group	0	0	0	1	2	0	3
Gunman	0	0	1	0	0	0	1
Hacker	13	5	9	15	11	15	68
Isis	0	0	1	0	0	1	2
Islamist	0	0	0	2	1	0	3

Jihadist	1	1	0	0	0	0	2
Journalist	0	0	2	0	0	1	3
Kidnapper	1	0	0	0	0	0	1
Killer	1	2	0	0	0	0	3
Mafia	0	0	0	0	0	1	1
Member	0	0	0	0	1	1	2
Molester	0	0	0	1	0	0	1
Nut	0	0	0	0	1	0	1
Offender	2	0	1	0	1	5	9
Operator	0	0	0	0	0	1	1
Paedophile	8	4	5	7	11	17	52
Peddler	1	0	0	0	0	0	1
Pervert	0	4	0	0	3	0	7
Player	1	0	0	0	0	0	1
Pornographer	1	0	0	0	0	1	2
Predator	1	1	1	0	0	0	3
Rapist	0	0	0	0	1	0	1
Recruiter	1	1	0	0	0	1	3
Reject	0	0	0	0	0	1	1
Researcher	0	0	2	0	1	1	4
Scientist	0	0	0	0	1	0	1
Seller	1	0	2	0	2	5	10
Smuggler	0	1	0	0	0	0	1
State	0	0	1	0	0	0	1

Student	0	1	0	0	1	2	4
Sucker	0	0	0	1	0	0	1
Suspect	2	2	1	1	1	0	7
Syndicate	0	1	0	0	0	0	1
Teenager	0	0	0	0	1	4	5
Terrorist	4	4	1	4	4	6	23
Thief	0	1	0	0	0	0	1
Trader	0	1	0	0	0	2	3
Trafficker	1	0	0	0	0	0	1
Troubled	0	0	0	0	1	0	1
User	7	4	15	11	4	24	65
Visitor	0	0	0	1	0	0	1
Whistle-blower	0	0	1	0	0	1	2
Youngster	0	1	0	0	0	0	1

The use of the term "criminal" is established in the media, with special emphasis by *The Times*, which applied this designation 34 times, thus representing 41.5% of the occurrences in this newspaper and 34.7% of the total. The first time that *The Times* applied this term was in November 2013, in the article "Dark internet site seeks funds to kill the president,"[116] where the crypto market Silk Road is presented as:

```
1 | A now-defunct site described 'like www.Amazon.com, but for criminals.'
```

[116] Related article: "Dark internet site seeks funds to kill the president," *The Times*, 20th November 2013, News, Page 12.

Although this website did actually connect drug dealers and users, it is important to remind the reader that chemical dependence is not per se a crime: '[A]n extensive survey of available data suggests that, contrary to popular belief, drug use and criminal behaviour are not causally related. It is also suggested that the use and abuse of drugs does not necessarily nor inevitably lead to crime' (Fink & Hyatt, 1978, p. 147). In the British press, the term "criminal" can define sellers and buyers, and the negative representation of addicts contributes to the moral panic in terms of drugs.

Another frequent name used by the British press is "hacker," with 68 occurrences, or 12.2% of the total. As noted by Jordan (2017, p. 27), 'hackers reveal or express in their practices the rationality of information technocultures by grappling constantly with their determinations and demonstrating where and how redetermination is possible and, accordingly, what the logics of information techno-cultures are even as they change and develop.' Coleman (2014, p. 59), who blames the media for the misinformation related to hacktivism and the stereotypes connected to the role, nevertheless maintains an optimistic view of this concept, in that 'hackers dedicate their lives and pour their souls into creating and programming the world's most sophisticated machines. They are quintessential craftsman—motivated by a desire for excellence.' Furthermore, the term "hacker" was initially related to the creativity involved in proposing innovative solutions to electrical engineering problems, and it was also connected to explorers of computer networks after the development of the Internet, but it went through a moral panic campaign 'in which the hacker appeared as a new kind of folk devil, recklessly invading networks, interrupting essential services, stealing state secrets or credit card numbers' (Wark, 2006, p. 321). The negative representation of hackers also entailed the development of the term "cracker" to refer to people using computer knowledge in an equally creative and innovative way but with criminal purposes (Wark, 2006). Jordan (2017, p. 14) discusses the golden age of cracking, affirming that 'a focus on cracking in police arrests and media publicity, along with a widening interest in "exploring" computer and network technologies, led during this period to a near identification of cracking and hacking.' The term "cracker," in fact, was never widely adopted by the media, as proven by the fact that it was never mentioned by the six researched newspapers. Moreover, Jordan (2009) argues that 'hackers and hacking offer both an important and complex

object and a way to rethink approaches to society, technology and socio–technological power.' Two quality newspapers, *The Daily Telegraph* and *The Times*, have 15 occurrences each of the term "hacker." A deeper analysis shows that this term is mostly used in connection with cybercrime. In *The Daily Telegraph*, for instance, it is used in the article "Hit men, drugs and the fall of the Silk Road 'mastermind,'"[117] in connection with the crypto market:

```
Computer hackers advertised services such as cracking into cash machines.
```

In an article issued by *The Times*, the term is also used in the headline "Hackers leak details of 1.2m Brits on adultery site,"[118] followed by the explanation:

```
In June, hackers accused Ashley Madison of having poor IT security. Impact Team
said that members who had paid to erase their profiles had not had their
information totally removed. A link to the data leak appeared yesterday on the
dark web, a part of the internet that is accessible only by using a special
browser.
```

Besides associating hackers with the Deep Web and the idea of a sophisticated knowledge of how to use it, this example also demonstrates the ethics in the context of hacker organisations, which target in their attacks companies that disrespect users' digital rights (Coleman, 2014).

Another term largely adopted is "user," with 65 occurrences, which represents 11.7% of the total. Although there is a distinction between recreational and instrumental users, the former being those who use the Internet mainly as entertainment and the latter those who focus on work or study (Liu, 2011), newspapers adopted the term "user" alone, as a neutral nomenclature, in the same way it is generally used in academic research. An example of how the Internet user could be potentially portrayed in a positive way instead of neutrally is the use of terms such as "netizen," ignored by the British press but which is broadly adopted in academic literature related

[117] Related article: "Hit men, drugs and the fall of the Silk Road 'mastermind,'" *The Daily Telegraph*, 5th October 2013, News, page 21.
[118] Related article: "Hackers leak details of 1.2 Brits on adultery site," *The Times*, 20th August 2015, News, page 7.

to a 'new form of citizen engagement enabled by the increase in digital technologies and the rise in the number of people who have access to the Internet' (Lindtner, 2014, p. 147).

Grouping these attributes by connotation, as seen in Table 13, highlights that negative uses of the Deep Web dominate the British press coverage. Interestingly, there are only negative and neutral attributes used to refer to Deep Web users, as the classification shows, and not even one positive designation used to describe them. It is worth mentioning here that for neutral, this research includes terms that can have positive or negative meanings according to the idea that is associated with it; the concept of "connoisseur," for instance, can be positive if connected to arts or wine, but negative if linked to drugs.

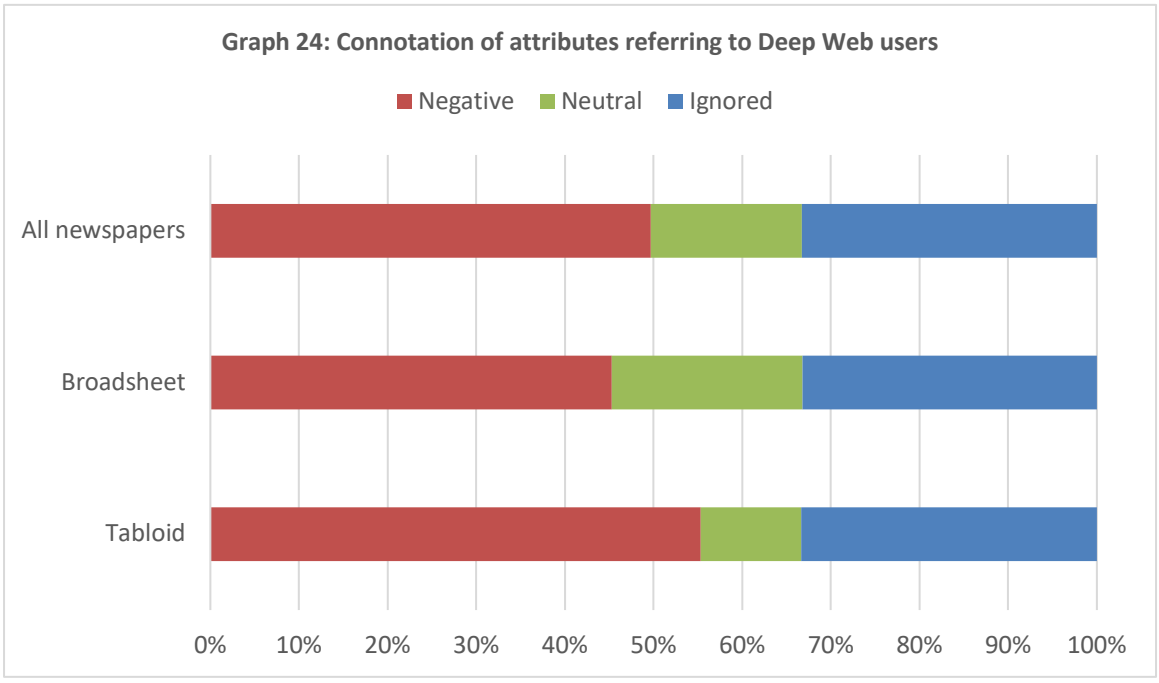
Table 13: Attributes connected to Deep Web users by connotation

CONNOTATION	ATTRIBUTES
Neutral	Activist
	Arab
	Backer
	Buyer
	Client
	Community
	Connoisseur
	Consumer
	Costumer
	Cryptographer
	Geek
	Government
	Group
	Islamist
	Journalist
	Member
	Operator
	Player
	Recruiter
	Researcher
	Scientist
	Seller
	State

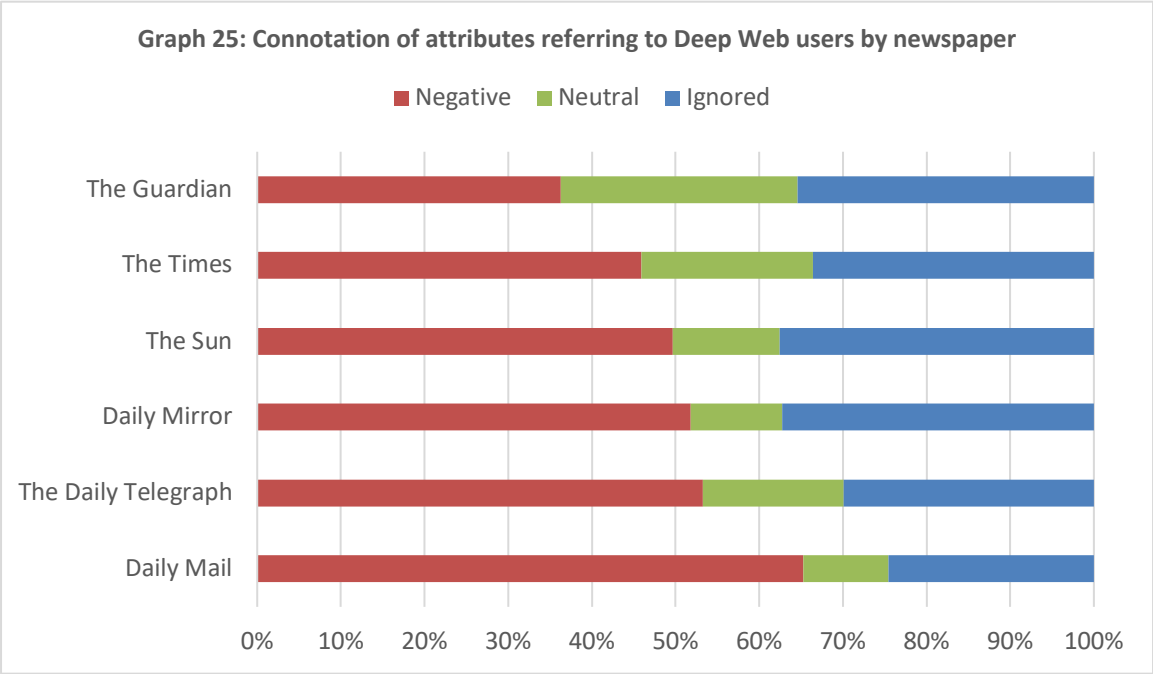
	Student Syndicate Teenager Trader User Visitor Whistle-blower Youngster
Negative	Abuser Addict Al-Qaeda Bomber Captor Conspirator Criminal Crook Cyber-villain Dealer Defendant Drug supplier Drug user Exploiter Extremist Fanatic Fiend Fraudster Gang Gunman Hacker Isis member Jihadist Kidnapper Killer Mafia Molester Nut Offender Paedophile Peddler Pervert

Pornographer
Predator
Rapist
Reject
Smuggler
Sucker
Suspect
Terrorist
Thief
Trafficker
Troubled

Using this classification, it is clear that, independently of the format, British newspapers vastly refer to Deep Web users in negative ways (see Graph 24). Tabloids, however, are more severe, with 55.3% of the attributes related to users considered as negative, while quality newspapers do the same in 45.2% of cases. Quality newspapers, in fact, expend some effort to use neutral attributes in order to refer to these users, with words such as "student," "member," "researcher" and "visitor." Moreover, only in quality newspapers can attributes be found which associate users with activism, as seen in the word "whistle-blower," for instance.



Taken separately, and not grouped by tabloid or quality format, it is clear that all the newspapers under examination contribute to some extent to the negative representation of Deep Web users. Graph 25 indicates, however, significant distinctions in their approaches. Tabloid and quality newspapers clearly occupy different places in the scenario, with the former being more emotional in their coverage. However, although *The Guardian* (moderate Liberal Democrat) is the newspaper with the highest number of neutral attributes, and therefore the most balanced one in this context, the percentage of negative associations is still considerable, with 36.3%. Conversely, *Daily Mail* (strong conservative) applies negative attributes in 65.3% of cases, an alarming number which undeniably proves the damaging framing of Deep Web users.



Another point to stress is that there are cases in which the articles not only link the Deep Web to criminal and antisocial behaviours, but also compare users of these technologies to general Internet users. In *Daily Mirror*, for instance, the term "normal web users"[119] is applied in

[119] Related article: "Drugs, guns, assassins, jet planes… All for sale on secret Deep Web; Internet can be scary but what lurks beneath is terrifying," Daily Mirror, 22nd September 2012, News, page 18.

opposition to Deep Web users. In this example, the word "normal" exposes the existence of a type of conformity related to how people are expected to engage with the Internet. In contrast, users with technical knowledge who employ distinct resources from the Deep Web, such as the Tor Network, are seen as anomalous, regardless of the reasons that led to their adoption. This rhetoric of opposing users increases the ongoing dichotomy between the two sides of the Web: arguing that just one side is normal, it not only disregards the fact that the Deep Web can have multiple positive uses, but also that the Surface Web can have a variety of negative ones.

From an additional perspective on how Deep Web users are portrayed by the British press, knowledge of this technology is also used to increase the panic surrounding historically targeted groups, such as Muslim minorities. Previous studies have shown that media representations of Islam are mainly connected to violence, concentrating on topics such as terrorism and war, and the rhetoric constantly situates Muslims as the "others" in the context of liberal societies, which contributes to Islamophobia (Ahmed & Matthes, 2017). In an article published by *The Sun*,[120] this negative portrayal of ethnicity is very obvious:

```
1 The terrified mum, 20, was warned she would be auctioned to Arabs on the dark
2 web – then fed to tigers when they grew bored.
```

In summary, independent of political stance and formats, newspapers provide a sharply negative representation of the Deep Web users, in that half of the time, they use nomenclatures that highlight criminal or antisocial uses, especially the terms "criminal" and "hacker." It is worth reiterating that there are no positive terms to define users, proving that the British press do not highlight positive uses. As noted by Dingledine (2010, p. 128), 'a privacy tool like Tor has many different classes of users around the world (ranging from ordinary people, civil rights enthusiasts human rights activists to corporations, law enforcement, and the military) so the fact that you have Tor installed doesn't give people much additional information about who you are or what sort of sites you might visit.' Considering the overall inclination of the media to portray the Deep Web in a negative manner, the way users are described corroborates the idea that using these

[120] Related article: "Brush with Black Death," The Sun, 7th August 2017, News, page 4.

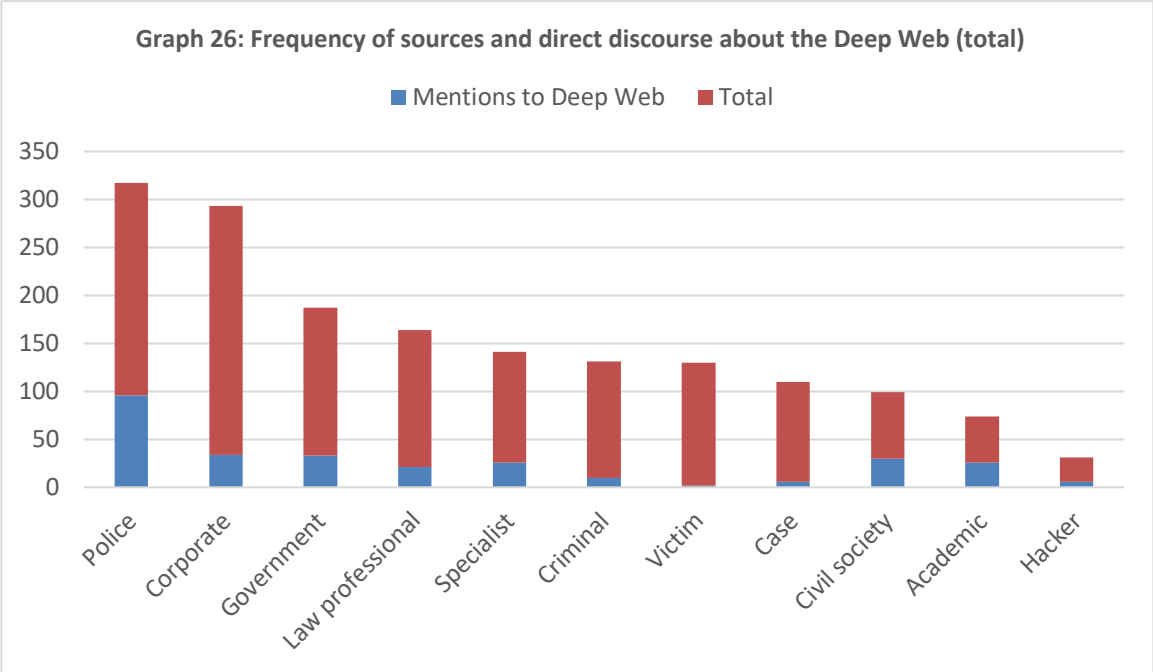
technologies is wrong and questionable, which contributes to a broader negative representation and the rise of panic.

5.6 Official Sources at the Centre of the Discourse

When analysing media production, the sources that are presented in the articles have the opportunity to speak their minds, and therefore their voices and viewpoints are privileged in relation to the ones that are absent, and their opinions shape the general representation of the topic (Kidd, 2016). Therefore, the variety of sources used in a newspaper article demonstrates the rhetorical approach to the topic, selecting ideas and attitudes to the issue. As this research compellingly argues, official sources such as government, police and law professionals are consistently used to promote the discourse against the Deep Web.

Considering the subject of crime in the media, for instance, public officials are persistently at the centre of the discourse, interpreting events, representing the dominant ideology and imposing their own definition of crime, since 'primary definers (i.e. law enforcement officials) succeed in establishing the terms of reference from which all discussion of crime emanates' (Welch et al., 1997, p. 475). Furthermore, the use of official sources by the media can be attributed not only to the news production logic, with constant pressure and short deadlines that induce the use of credible sources commonly represented by police and government, but also to the own idea that the matter needs formal confirmation or validation by the institutions (Welch et al., 1997).

This content analysis measured the sources used in the British newspaper articles about the Deep Web and to what extent these sources provide a direct comment about these technologies. Among the findings, this research unveils that official sources – representatives of police and government – account for 30.1% of the voices in the articles and for 44.5% of the opinions that are directly related to the topic (Graph 26).



In the case of the police, responsible at the same time for the highest number of sources and opinions (see Graph 26), it is possible to say that the overall discourse of this institution not only connects the Deep Web to crimes, but it also frames it generally as a threat. This attitude can be seen in any of the researched newspapers. In an article published in *The Times*,[121] for instance, Lee Miles, deputy head of the National Crime Agency (NCA) National Cyber Crime Unit, says:

```
People think some spaces are 'no-go' areas [for police] but, while they are
very challenging, investigations like the Silk Road show that we operate in
places of interest that some people regard as untouchable. We can tackle these
areas and we are continuing to do that in areas which we think pose the
greatest threat.
```

An article from *The Daily Telegraph*,[122] a source also from NCA associates the "hidden web" with violence, mentioning that:

[121] Related article: "Drugs and weapons are still for sale on 'dark net,'" The Times, 25th November 2013, News, page 1.
[122] Related article: "Rising threat of child abuse, drugs and guns," The Daily Telegraph, 1st May 2014, News, page 2.

```
Criminals will increasingly exploit legitimate channels for bringing guns into
the country, and these could be used by terrorists.
```

In *The Guardian*,[123] another source from NCA reassures the power of the police, stating that:

```
Criminals like to think that the dark web provides a safe, anonymous haven but
in reality this is just like any other organised crime network. It may take
time and effort to investigate and build a criminal case, but we are determined
to identify and prosecute people caught dealing drugs and committing serious
crime using the dark web.
```

Taking also cases from tabloids, an article in *The Sun*[124] presents a representative of the FBI as a source, to raise concerns about Silk Road, mentioning that it is:

```
The most sophisticated and extensive criminal marketplace in the Internet
today.
```

An example from *Daily Mirror*[125] shows the connection between the Deep Web and child pornography, with a source saying that the focus of investment and investigation of the Irish Garda is paedophiles, because they are:

```
More determined to access child porn through the dark net, a hidden corner of
the internet which makes it hard to track down user addresses.
```

On the same matter, an article from *Daily Mail*[126] uses a source connected to the Child Exploitation and Online Protection Centre of NCA to talk about "sick websites," noting that:

```
Hard-core paedophiles don't go onto Google to search for images. They go onto
```

[123] Related article: "Six Britons arrested over Silk Road 2.0 amid dark-web takedown," The Guardian, 8th November 2014, Technology, page 13.
[124] Related article: "FBI shut hitmen & drugs site," The Sun, 3rd October 2013, News, page 2.
[125] Related article: "Web firm to block kid porn," Daily Mirror, 11th November 2014, News, page 13.
[126] Related article: "It's not just child porn," Daily Mail, 23rd November 2013.

```
the dark corners of the Internet.
```

Therefore, the general rhetoric of the police in the newspapers, be it tabloid or quality, sharply connects these technologies to negative uses. The reason why official sources are broadly presented in the articles is because the panic rhetoric requires from authorities a position on a specific matter, which can even lead in some cases to the creation of new laws (Cohen, 2011). This negative attitude can be seen in an example from *The Times*[127] showing former British Prime Minister David Cameron talking about Deep Web users as:

```
Polluted minds hidden in the darkest corners of the internet.
```

This sentence not only relegates the use of these technologies to problematic behaviour, but also questions the very existence of covert access to the Internet. However, authorities are not always this emotional and pessimistic when addressing the subject. In an article[128] published in the same newspaper in 2012, for instance, a US State Department spokesperson states:

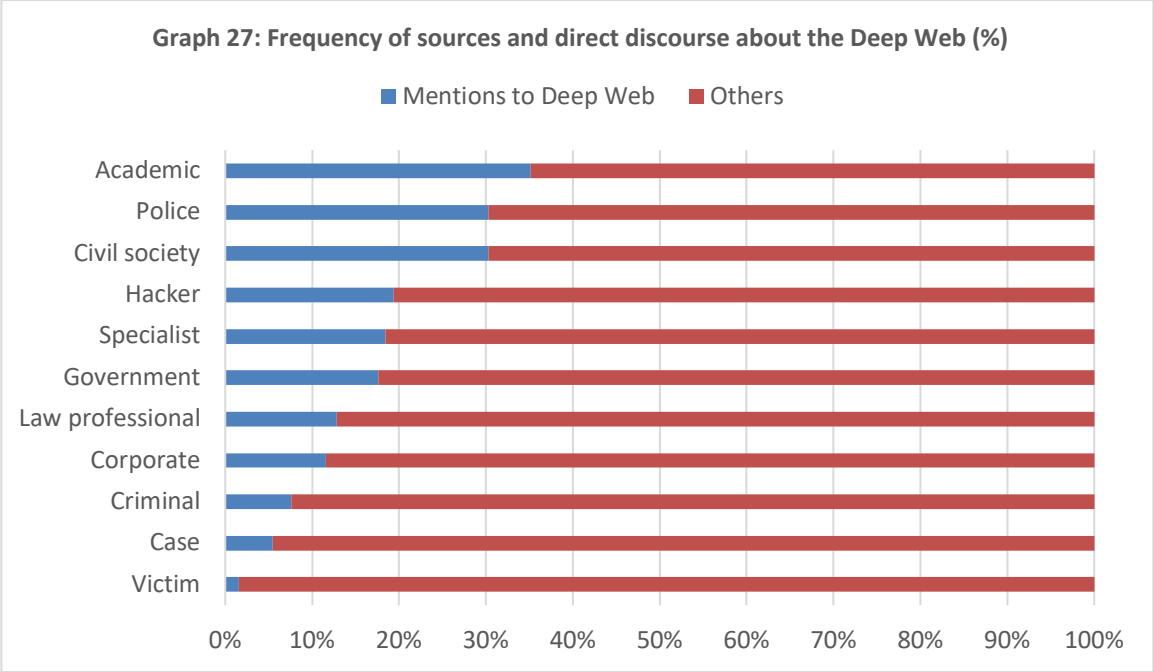
```
Tor is one of several technological tools that the Department of State helps
develop to enable activists in repressive environments to safely exercise their
rights to free expression, free assembly and free association online. Like any
technology it can be used for good or ill ends.
```

Analysing the numbers related to sources from the perspective of the percentage making a direct comment about the Deep Web (see Graph 27) allows us to conclude that although academics are not the preferred source, with just 4.4% of the total, they are more likely to give an opinion, which happens in 35.1% of the cases. This is evident in the article "CSI's real-life fighter against cybercrime,"[129] published by *The Daily Telegraph* and in which the main source is

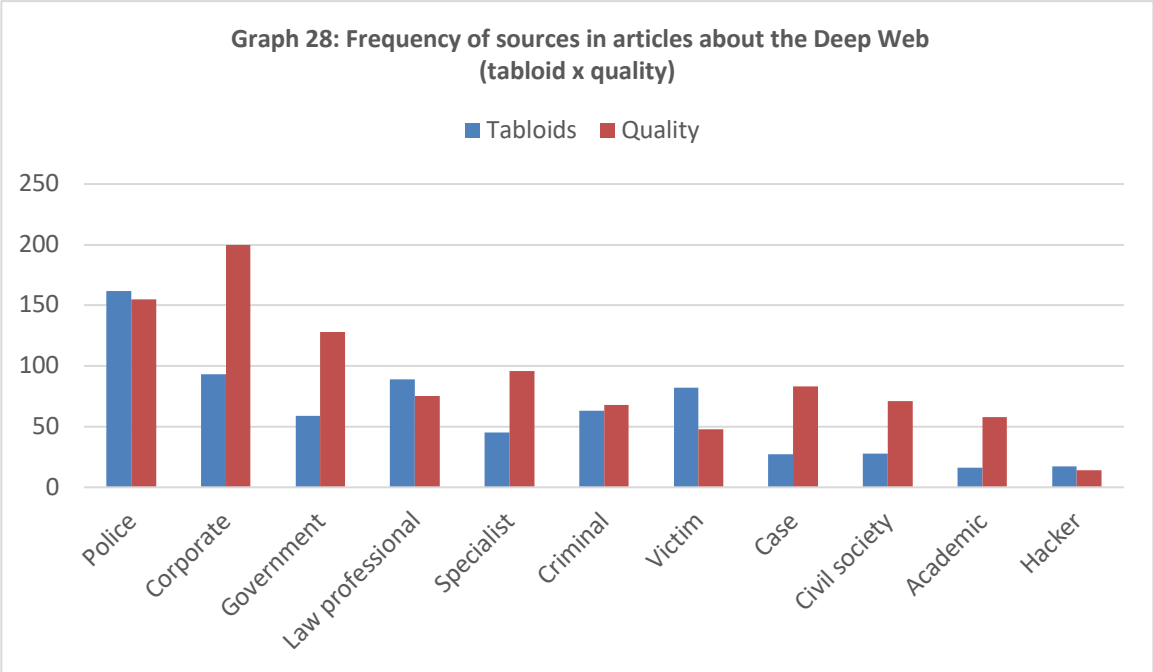
[127] Related article: "Internet to face same restrictions as sex shops," The Times, 22nd July 2013, News, page 2.
[128] Related article: "Drugs, guns and passports for sale on Dark Web," The Times, 3rd April 2012, News, page 12.
[129] Related article: "CSI's real-life fighter against cybercrime," The Daily Telegraph, 4th November 2015, Features, page 26.

Professor Mary Aiken, director of the Cyber-Psychology Research Centre at the Royal College of Surgeons in Dublin. She offers a sensible view on the matter of the Deep Web, saying that:

```
Technology itself is not good or bad, it is either used well or poorly by
humans.
```



Comparing the use of sources among newspapers with distinct natures (see Graph 28), one point to highlight is that from a total of 1,677 sources used in the articles, tabloids account for 40.6% of them, while quality newspapers are responsible for the other 59.4%. In the context of the role of the print media in fear production, tabloids occupy a special role, since these newspapers have a journalistic approach centred on popularisation, personalisation and sensationalism, with 'more extensive use of narratives and more limited use of an analytical mode, as well as greater emphasis on personal and human interest stories' (Skovsgaard, 2014, p. 202). Quality newspapers, being essentially more analytical, are more likely to present a broader number of sources and offer contrasting opinions.



The limited use of hacker groups as sources, in contrast with considerable links to the Deep Web, shows the discrepancy between newspapers attributing criminal practices to hackers but not revealing their perspective in the articles. On the one hand, hackers represent only 1.8% of the total sources, with 17 occurrences in tabloids and 14 in quality newspapers, which shows little effort in giving them a voice. And on the other hand, Deep Web users are called "hackers" 12.2% of the time – this term occupies the second position in numbers of occurrences among all terms describing users. This discursive approach not only increases the negative connotation of the term, which is already surrounded by misinformation and stereotypes (Coleman, 2014), but it also perpetrates an idea of technical knowledge being inadequate per se, since hackers are consistently blamed for the misuse of technology.

In addition, it is interesting to note that *The Times* is the only newspaper that mentioned having attempted to contact these groups; in the rest of the cases, newspapers that do not present the side of these groups also do not mention attempting to do so. In April 2012, however,

an article about the crypto market Silk Road, entitled "Drugs, guns and passports for sale in Dark Web,"[130] mentioned that:

```
Representatives for Silk Road declined to comment.
```

Again, in January 2015, the article "Military secrets for sale on dark web,"[131] about the development of the crypto market The Slur by the u99 group, a website dealing in the trade of confidential information about governments and corporations, mentions that:

```
The u99 group did not respond to request for comment.
```

The fact that there are only two cases in which an attempt to contact is mentioned from a total of 833 articles can be seen from a positive perspective, i.e. as a legitimate effort to give a voice to hacker groups, or as a cynical way in which a sentence is inserted into the article to lead the reader to think that the newspaper has an unbiased approach when trying to contact these groups, but contact is actually unfeasible.

In addition, the second most-used source in the articles is categorised as corporate, with 17.5% of the total. This includes professionals in multiple fields that are consulted because of their connection with the company whose name is mentioned in the article, such as executives or consultants from technology corporations. These sources are mostly used to explain the technical aspects of the Deep Web, thereby providing a layer of sophistication to the technology and justifying authorities' efforts against it. In one such example from *The Daily Telegraph*, the article "Cameron wins FBI support for 'dark web' war on paedophiles"[132] includes the following extract:

```
Joanna Shields, who runs 'Tech City,' a cluster of technology operations in
London, has been asked to lead a group of senior industry figures to explore
possible solutions to help break through the encryption of the dark web. She
```

[130] Related article: "Drugs, guns and passports for sale on Dark Web," The Times, 3rd April 2012, News, page 12.
[131] Related article: "Military secrets for sale on dark web," The Times, 14th January 2015, News, page 15.
[132] Related article: "Cameron wins FBI support for 'dark web' war on paedophiles," The Daily Telegraph, 18th November 2013, News, page 2.

```
said: 'It is vital that governments and industry work together to eradicate
child abuse content from the internet, and that we mobilise the best and
brightest in the technology industry to come up with innovative solutions to
tackling this problem.'
```

Interestingly, British newspapers also give the same space to preparators or suspects and victims of crime. This research includes as "criminal" sources that committed the crime or are being accused of committing or planning a crime, and as "victim" sources who were personally impaired by a crime connected with the Deep Web's functionalities. Both sources each have a total of 7.8% representativeness, which indicates that both sides are equally portrayed. Looking at the newspapers according with their nature, however, there is a difference between tabloids – which focus more on victims (12.0%) than on criminals (9.3%) – and quality newspapers – with criminals (6.8%) having more space than victims (4.8%). Hence, this validates the idea that tabloid newspapers use personal experiences to trigger discussions about security and society (Iyengar, 1990).

The remaining sources used by the newspapers are less representative. Specialist, for instance, refers to people consulted because of their professional knowledge, such as IT consultants, cyber security experts, researchers and other professionals, but including only cases in which the related company is not cited. They represent 8.4% of the sample. With 6.6% of occurrences, the category "case" is used when a random source has a voice in the article but only to exemplify something related to the main topic. Finally, "civil society organisations," at 5.9% of the cases, are groups that advocate for civil rights, other civil organisations, charities, activists, religious congregations and think-tanks.

5.7 Discussion: Hyper-panic, when Media Panic meets Moral Panic

As this chapter argues, the British press contribute to the fear-producing logic that surrounds the Deep Web imaginary through a negative representation of these technologies connecting them to well-known social anxieties. This combination of fears is conceptualised as hyper-panic, namely when a new medium, such as the Deep Web, enables or facilitates threats such as child abuse, terrorism and trade in drugs. In relation to the panic about a new medium's potential, this

chapter demonstrates that there is a fear related to the Deep Web's affordances and how these technologies can increase risks that the Internet already offers. For instance, privacy-granting technologies allow online anonymity, which can have negative uses (Larsson et al., 2012; Martin, 2014; Morselli et al., 2017; van Hardeveld et al., 2017). In addition, there is a fear related to these technologies' opacity, since newspapers offer limited and superficial discussions, helping to keep the status quo in terms of the general lack of technical knowledge about how they work. Moreover, the British press address the Deep Web mainly in terms of negative uses, such as propagating the misleading idea that criminals are the majority of users of these technologies and that there are no positive uses, a notion broadly contested by academic research (Dingledine, 2010; Hoang & Pishva, 2014; McLeod, 2011; Moore & Rid, 2016; Sharon & John, 2018; Wu & Atkin, 2018).

This work identifies four aspects through which the British press connect the Deep Web to social anxieties contributing to a negative representation of these technologies, and which are seen as undesirable, immoral or illegal: offering episodic coverage, making negative associations in headlines, labelling users and resourcing mostly to official sources. While addressing privacy-enhancing technologies, newspapers practice episodic coverage characterised by punctual increases in the amount of publications on selected events involving antisocial and criminal behaviours, such as paedophilia, drugs and other crimes. Furthermore, the general discourse of the headlines ascribes associations with negative behaviours, using a sharply detrimental and emotional rhetoric. In terms of users, British newspapers predominantly apply negative terms, especially connecting them to criminal or antisocial activities. This logic that the Deep Web is mostly in the news because of negative uses leads to the conclusion that these technologies multiply existing fears. Adding to this point, newspapers afford more significance to official sources' discourse, mainly the government and police, focusing on these authorities' plans and actions to fight the Deep Web, thus helping to build an adverse representation of these technologies.

Although privacy-granting technologies and the Deep Web allow multiple uses, from freedom of speech to bullying (Jardine, 2018a), the British press visibly portray them as the main source of immorality on the Internet, as Gehl (2016) assumed. An article of *Daily Mirror* entitled "Evil of

Dark Web"[133] illustrates that these technologies are used by "smugglers" for "disturbing" reasons and "under the radar of traditional law enforcement." An example in *The Sun*[134] shows an attempt to ensure the polarisation of the Web:

> There's no doubt the Internet has done wonderful things for the world and remains one of the greatest inventions since the wheel. But it also means that the ingredients for new hardcore designer drugs can be posted online and then made up by almost anyone.

Stressing mostly criminal uses, this example illustrates the commonest approach seen in the press daily coverage, i.e. raising fears about the potential use of a new medium (Drotner, 1999). While the Deep Web is still relatively unknown to the average user and has the potential to help people protect their privacy from corporate and state surveillance (Bellare & Rogaway, 2005; Dingledine et al., 2004; Floridi, 2014; Jardine, 2018b; McCoy et al., 2008; Moore & Rid, 2016), the British press incessantly represent it as a negative platform. As Drotner (1999, p. 618) contends, 'critics of new media continue their allegations of crime despite commission reports and empirical studies. That is also why direct behaviourist explanations of media effects retain their currency in the panic despite theoretical developments.' Considering that the Deep Web, and in particular the Tor Network, has a number of legitimate uses related to freedom of speech (Jardine, 2018b) and the safe communication of sensitive topics (McLeod, 2011; Sharon & John, 2018; Wu & Atkin, 2018), it is alarming that the British press have a very limited intention to educate people on this matter. This research demonstrates that higher circulation newspapers in the United Kingdom barely attempt to raise awareness about online privacy and state and corporate surveillance issues that affect people's everyday life, as well as cybercrime.

Criminality is not caused by technology per se, since people can use the same technology in multiple ways (Lum, Koper & Willis, 2017); for example, criminals can resort to privacy-enhancing software to commit offences, and authorities can apply the same tool to understand better their communities and fight crime. Certainly, there is an aspect of technological development that

[133] Related article: "Evil of Dark Web," Daily Mirror, 6th August 2017, News, Page 12.
[134] Related article: "Drug horror," The Sun, 21st January 2016, Editorial, page 8.

adds sophistication to cybercrime (Larsson et al., 2012; Martin, 2014; Morselli et al., 2017; van Hardeveld et al., 2017), but it is also used to protect people's right to private communication and access to information (Floridi, 2014; Hoang & Pishva, 2014; Jardine, 2018b; McLeod, 2011; Sharon & John, 2018; Wu & Atkin, 2018). Nonetheless, this relevant discussion is somewhat unusual in the British press, which invest time and paper discussing technical advances that can facilitate illegalities filled with negative representations of the Deep Web systems, users and uses. This leaves limited space to reflect on the multiple possible uses of the Web or to debate the reasons why people become criminals, how the online drugs trade can affect society, why people should protect themselves online and other topics on the Deep Web's legal or illegal uses. Therefore, newspapers blame the Deep Web for all online evil, making people fear not only these technologies, but also their users in general, thereby ignoring legitimate practices that could contribute to a more democratic society. Actually, they do the opposite, by constantly focusing on negative aspects, keeping explanations to a superficial level and contributing with a biased imaginary that scares people away.

6 The Tor Network and the Dream of Online Freedom

Artificial intelligence, virtual reality, robots, smartphones, computers: these and other new technologies have in common the ability to raise hopes and fears in the world. Mansell (2012) claims that technological innovations introduced into the information society can be, on the one hand, an outsider shock and, on the other hand, perceived as a potential contributor in positive changes to inside dynamics. Furthermore, public responses to new technologies usually vary, from dreams to nightmares (Malbreil, 2007), hope to fear (Sturken et al., 2004; Natale & Ballatore, 2014), positive to negative views (Barney et al., 2016; Bartlett, 2015; Coleman, 2014), euphoria to resistance (Paulus et al., 2013), sublime to demonisation (Mosco, 2004). A similar dichotomy is seen in the British press's representation of the Tor Network, as this chapter outlines.

The previous chapters provide compelling evidence that Deep Web technologies, uses and users are represented in a dramatically damaging way by the British press. Empirical research shows that the Deep Web is mainly portrayed as negative, inexplicable and opaque. Moreover, it is seen as a threat and is constantly associated with several social fears, a process that this thesis conceptualises as "hyper-panic." This chapter, however, focuses on the particular case of positive representations of the Tor Network, the best-known Deep Web technology (Bartlett, 2015; Dingledine et al., 2004; Moore & Rid, 2016; Sui et al., 2015). It achieves this by looking at cases in which British newspapers describe Tor in affirmative tones, in order to understand the arguments used by the media while addressing the benefits of a privacy-enhancing technology as a means of accomplishing online freedom. Beyond misinterpretations and threats, this work unveils nuances in the media discourse: do the British press contribute to keeping the dream of a free cyberspace alive? Does the news show Tor as a liberating technology for those who want a free and safe Web? How do newspapers actively introduce a good perspective on Tor?

This analysis presents findings following the examination of 17 newspaper articles discussing Tor in a positive tone, using a combination of content analysis and critical discourse analysis. This sample was retrieved from the total of 833 publications analysed in this empirical research, considering those articles using terms such as "Tor," "Tor Browser," "the Tor Network" or "Tor

System" in the six analysed newspapers – *Daily Mail*, *Daily Mirror*, *The Sun*, *The Daily Telegraph*, *The Guardian* and *The Times*. As explained in the *Methodological Framework* chapter, these keywords were included in the original search for articles through Nexis. The time frame is a period of 10 years (2008-2017), since only in 2008 was the first article about Tor published by these newspapers. Finally, this sample includes only those articles looking exclusively at the positive uses of Tor. The limited number of publications allows this research to draw a critical discourse analysis that looks into the detail and provides insights that contribute to a better understanding of how the British press represent technology in general.

To understand to what extent Tor is seen by British newspapers as a liberation technology, this chapter focuses initially on understanding the concept in the context of the Web, providing a discussion about how technology is represented overall. Considering Tor as a contemporary manifestation of liberation technology ideals (Chouliaraki, 2010; Ziccardi, 2013), an overview of its self-mediation provides insights into which attributes and purposes are committed to promoting freedom (Cammaerts, 2015), and therefore what aspects make Tor a liberation technology. Additionally, the following sections discuss how the libertarian argument is presented by the press, including uses that Tor enables, such as whistle-blowing and other forms of activism. In the final discussion, this chapter provides insights related to Tor's representation and newspapers' approaches to issues related to surveillance and privacy.

6.1 On the Concept of Liberation Technology

Shortly after the invention of the Web, Negroponte (1995, p. 229) explored an enthusiastic argument in favour of this technology despite an undesirable and latent dark side: '[B]eing digital, nevertheless, does give much cause for optimism. Like a force of nature, the digital age cannot be denied or stopped. It has four very powerful qualities that will result in its ultimate triumph: decentralizing, globalizing, harmonizing and empowering.' The quality related to empowerment connected to the technology's potential, according to Negroponte (1995, p. 231), is the most relevant example, since digital enables 'a global information resource' and also 'the access, the mobility, and the ability of effect change are what will make the future so different from the present.' In this bright future that Negroponte (1995) pictured more than 20 years ago, when the

Web was surrounded by predictions, ensuing generations would be more and more digital, and the world would have far less spatial limitations for the circulation of knowledge. Hence, Negroponte (1995) contended that digital was at the centre of positive changes in the world. According to McLuhan (1964, p. 7), 'the medium is the message […] For the "message" of any medium or technology is the change of scale or pace or pattern that it introduces into human affairs.' As such, technology defines transformations in societies. Both scholars had a deterministic approach to technology.

Considering that 'technological determinism is the claim that the nature of a particular technology determines the nature of society' (Jordan, 2008, p. 13), a common criticism of this notion involves contemplating technologies as 'socially conditioned in their invention, construction and forms of use.' In this sense, the aim of technologies is to help fix problems and meet social needs (Jordan, 2008). Williams (1975, p. 31) criticises technological determinism by discussing interpretations of the relationship between society and technology. Regarding television, 'when there has been such heavy investment in a particular model of social communications, there is a restraining complex of financial institutions, of cultural expectations and of specific technical developments, which though it can be seen, superficially, as the effect of a technology is in fact a social complex of a new and central kind.' For Jones (1998, p. 13), on the development of the Web, 'current discussions of this "new medium" frequently fail to distinguish between technical inventions (digitalization of data and its means of transmission), the socially instituted technology ("the Internet") and its attendant cultural forms (email, websites, reactive and interactional interactivity, etc.).' As a result, understanding technology as a central point of transformation in societies seems an oversimplification, since 'changing technology will always be only one factor amongst many others: political, economic, cultural, and so on' (MacKenzie & Wajcman, 1999, p. 3).

Criticising technological determinism, however, is different from ignoring optimistic views of the Web as an instrument of emancipation, an approach that survives to the present day. Diamond (2012, p. 4) argues that the Internet has the ability to 'empower individuals, facilitate independent communication and mobilization, and strengthen an emergent civil society,' since it 'enables citizens to report news, expose wrongdoing, express opinions, mobilize protest,

monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom.' Furthermore, technological empowerment affords benefits in multiple situations. In the context of gender studies, for instance, information and communication technologies (ICTs) are fundamental in promoting the economic development and independence of women (Pardhasaradhi & Rao, 2014). In the context of labour, positioning the workforce as central, and adopting technologies that support their activities and enable articulation, can motivate a more democratic environment (Berg, 1998). From an additional perspective, online technologies provide relevant tools for political involvement, while emancipation facilitates awareness and participation (Pirannejad & Janssen, 2019).

In general, technologies are developed 'to improve our existence, to make our lives easier, to save time. Technology, then, appears to be the solution to a problem. We use technology to enhance ourselves, to magnify our force or efficacy, usually for purposes or environmental adaptation or control' (Matthewman, 2011, p. 12). Related to information and communication technologies (ICT), they are considered to have multiple agencies; software, for instance, 'forbids some things and allows others – this is seen as the virtual and effective equivalent of barriers and tolls, walls and fences' (Matthewman, 2011, p. 12). Beyond this notion, thinking about the Web as an instrument of empowerment is directly related to the idea of liberation technology, which Diamond (2012, p. 4) defines as 'any form of information and communication technology (ICT) that can expand political, social, and economic freedom. In the contemporary era, it means essentially the modern, interrelated forms of digital ICTs – the computer, the Internet, the mobile phone, and countless innovative applications for them, including 'new social media' such as Facebook and Twitter.'

In the case of the Internet, these ideals of liberation and freedom are directly related to access to knowledge and multiple viewpoints (Diamond, 2012). On several occasions, the inventor of the Web, the British engineer and computer scientist Tim Berners-Lee, openly acknowledged that the idea behind the development of the technology is the same as that which is defined as liberation ideology. In 1998, for instance, the Web inventor said that 'people have often asked me whether the Web design was influenced by Unitarian Universalist philosophy. I have to say that it wasn't explicitly, as I developed the Web well before I came across Unitarian

Universalism at all. But looking back on it, I suppose that there are some parallels between the philosophies.'[135] It is worth considering here that Unitarian Universalism[136] is considered a liberal religion which defends seven principles 'within a "living tradition" of wisdom and spirituality, drawn from sources as diverse as science, poetry, scripture, and personal experience.' The most important principle, which commonly summarises their philosophy, is the fourth, namely 'a free and responsible search for truth and meaning.'

In a recent interview with *The Guardian*, Berners-Lee responded to critics, reaffirming that 'the web is for everyone, and collectively we hold the power to change it. It won't be easy. But if we dream a little and work a lot, we can get the web we want.'[137] Furthermore, this view of technology as a collective construction is part of an argument which has significant momentum in "A Declaration of the Independence of Cyberspace," published in 1996 by the Electronic Frontier Foundation for the North American poet and Internet philosopher John Perry Barlow. In his statement, Barlow says that 'we are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.'[138]

Today, however, the Web is a central piece in a culture of surveillance in which giant corporations profit from collecting private data and selling this information to third parties, which is tolerated by users because of the benefits of online services such as email, social media, web mapping, exercise trackers and others (Lyon, 2018). Furthermore, online privacy is vulnerable not only to the external actions of technology companies (Striphas, 2015) and governments (Greenwald, 2014), but also personal interests, influenced by hacking activity as one example (Landau, 2017). In this context of surveillance and censorship, the association of the Web with the idea of liberation technology resists through specific initiatives as well as technical resistance tactics, such as the Tor Network (Ziccardi, 2013).

---

[135] Available on https://www.w3.org/People/Berners-Lee/UU.html Access: June 2019.
[136] Available on https://www.uua.org/beliefs/what-we-believe/principles Access: June 2019.
[137] Available on https://www.theguardian.com/technology/2019/mar/12/tim-berners-lee-on-30-years-of-the-web-if-we-dream-a-little-we-can-get-the-web-we-want Access: June 2019.
[138] Available on https://www.eff.org/cyberspace-independence Access: June 2019.

Surveillance issues are related to civil liberties. The right to privacy, for instance, is the 'freedom of personal autonomy, the most obvious being freedom of choice' as well as 'a freedom from unwarranted intrusion, surveillance and intimidation' (Miller, 2011, p. 114). The protection of freedom through enabling privacy is one of Tor's purposes and mainstream uses. From the technical perspective, Tor offers users layers of encryption which provide encrypted pathways to Internet access and assure a private connection (McCoy et al*.,* 2008). For this reason, Tor is considered by many as the best available tool to achieve anonymous communications online (Hoang & Pishva, 2014). From the sociological angle, Tor is a useful instrument for allowing a level of anonymity for Internet users (Sui et al*.,* 2015), thus making it a relevant resource, due to the massive level of surveillance of contemporary societies (Jaeger, 2015). Furthermore, the academic discussion about Tor constantly acknowledges that the online anonymity allowed by the network provides a freedom which is functionally neutral and adopted in multiple positive and negative ways (Jardine, 2018b).

In addition, discussions about Silk Road, the most famous crypto market on the Deep Web and accessible only through Tor, are often connected to a liberation ideology. Discussing engagement with online communities for research purposes, and using the example of Silk Road, Barratt & Maddox (2016, p. 704) posit that 'cryptomarkets [sic] are a recent socio-technical innovation, aligned with an ethos of information liberation, that provide autonomous market activity outside of the centralized control of governments.' Also, using the example of Silk Road to argue that crypto markets are libertarian counter-conduct of resistance, Sotirakopoulos (2018, p. 190) notes that 'trade in the dark net has been viewed by some enthusiasts as an example of how an unhampered and free market that keeps the distortions of the state's regulations at arm's length can be a viable model that should be expanded in more and more social spheres.'

Finally, British newspapers usually ignore the fact that Tor is used for privacy reasons, i.e. as a liberation technology and as a way of getting online anonymity and avoiding digital surveillance, missing the point that it is actually a response to this vigilance's ubiquity that affects individual online behaviour and leads citizens to adopt privacy-granting technologies as a protective measure (Jardine, 2018b). Moreover, Tor is a critical instrument against the ongoing expansion of surveillance and censorship practices over the Internet, promoted by governments and

corporations worldwide in order to control data (Lyon, 2009). Developed to give power to Internet users independently of the political situation, i.e. democratic or undemocratic, Tor is a contemporary manifestation of the liberation technology discourse.

Furthermore, portraying the Tor Network as a new manifestation of the technological liberation argument, as seen in Ziccardi (2013), is the core of Tor's self-mediation, which is the 'empowering potential of new media technologies to invent novel discourses of counter-institutional subversion and collective activism' (Chouliaraki, 2010). Moreover, the overall discourse available on The Tor Project website and social media accounts presents values related to freedom and emancipation, as the following overview shows. Through these ideals, Tor builds an imaginary of the technology as a resource against censorship, since self-mediation is 'a dialectical, communicative process that encompasses but also complicates a variety of dichotomies; the production of media and symbols versus their reception or use, alternative media versus mainstream media, traditional media versus new media, and the symbolic versus the material' (Cammaerts, 2015, p. 1). This research resorts to The Tor Project's website as well as official social media accounts, to understand the conversation used to define this technology.

'Browse Privately. Explore Freely' is the slogan of The Tor Project[139], followed by 'defend yourself against tracking and surveillance. Circumvent censorship. Download Tor Browser.' Furthermore, the main issues related to surveillance studies are mentioned in these lines – "privacy," "freedom," "surveillance," "tracking" and "censorship." They are repeated on the homepage, when the mission of the initiative is specified, namely to 'advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding.' Considering the definition provided by The Tor Project, this technology is clearly described in an optimistic and positive way as an obvious solution to privacy concerns, an enthusiastic approach to technology empowering users that can be compared to Negroponte's (1995) views of the Web.

[139] Available on https://www.torproject.org/ Access: May 2019.

One of the minds behind the development of Tor, Dingledine (2010), organised the following list of 10 rules for choosing a privacy-granting tool: (1) a diverse set of users; (2) availability in the country; (3) sustainable network and software development strategy; (4) open design; (5) decentralised architecture; (6) protection against website tracking; (7) clear communication with no false promises; (8) consistently good latency and throughput; (9) easy-to-access software and updates and (10) doesn't promote itself as a circumvention tool. All of these items are seen in Tor's self-mediation, but specially the last one. Tor's image is impaired by potential negative uses, so it is expected to avoid attracting people that want to use Tor to commit crime and avoid the law. In practice, there is an effort to introduce "Tor primarily as a privacy and civil liberties tool rather than a circumvention tool" (Dingledine, 2010, p. 6).

On the matter of Tor's purposes, the website includes the following: blocking trackers, defending against surveillance, resisting fingerprinting, multi-layered encryption and browsing freely. According to Chopra & Dexter (2007, p. xiii), the development and popularisation of software in the twentieth century, contributing to the promise of a more democratised control of new technologies, motivated strong responses which were seen as 'an attempt to embrace and co-opt this control to advance entrenched social, economic, and political power. It is this reaction that free software resists.' Chopra & Dexter (2007) suggest that online technologies and ideals around freedom have been connected since the very beginning of discussions on the Internet, but the emergence of free software clearly exemplifies concrete action to use technologies' potential and act as a force for liberation purposes. In the case of Tor, this can be seen in the following argument: '[W]e believe everyone should be able to explore the internet with privacy. We are The Tor Project, a 501(c)3 US non-profit. We advance human rights and defend your privacy online through free software and open networks.'

The overall message sent by The Tor Project through its social media presence is that the software embraces the challenge of protecting people's rights. This can be consistently identified in posts collected from their Instagram account[140] (see Figures 13 to 16). In Figure 13, for instance, a post published in December 2018 presents two articles of the Universal Declaration

[140] Available on https://www.instagram.com/torproject/ Access: May 2019.

of Human Rights with highlighted sentences. The first is related to the right to privacy, and the second refers to the right to freedom of speech. In addition, the image has the following caption: '[T]he universal human rights to privacy and freedom online must be defended. Tor is a critical tool in this fight.' In this context, Tor is presented as a viable option to achieve civil liberties.

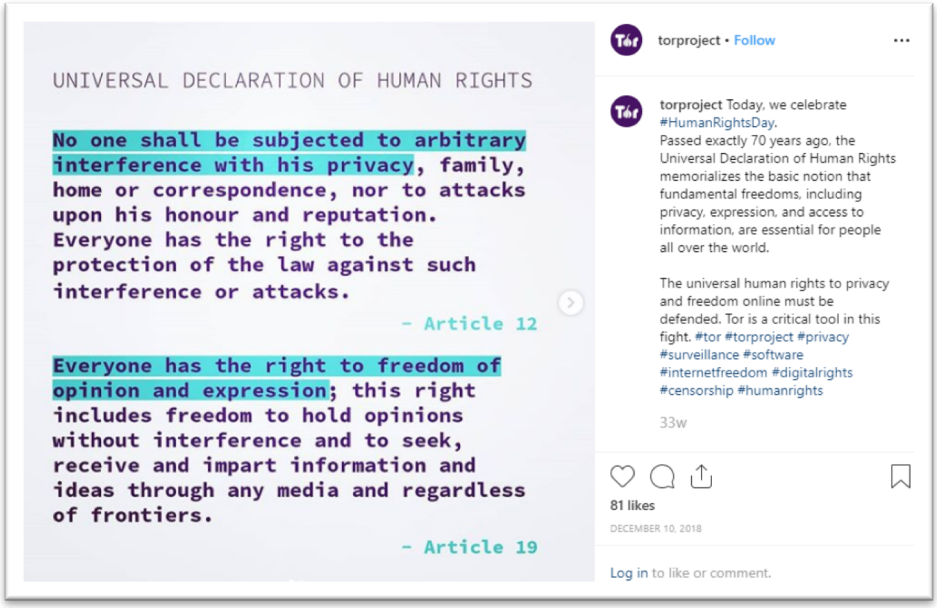


Figure 13: Post by The Tor Project: Universal Declaration of Human Rights (10th December 2018)
Source: The Tor Project Instagram account (@TorProject)
Retrieved by the author in May 2019

In another example, Figure 14 includes sentences from a speech made at the 2018 Human Rights Council about how privacy-enhancing technologies such as Tor empower people looking for knowledge and discussing ideas, since it minimises the fear of retaliation. In 1997, talking about the original dream of the Web, Berners-Lee said that 'in a world of people and information, the people and information should be in some kind of equilibrium. Anything in the Web can be quickly learned by a person and any knowledge you see as being missing from the Web can be quickly added. The Web should be a medium for the communication between people: communication through shared knowledge.'[141] Interpreting the Instagram post through this ideal purpose mentioned by Berners-Lee, on the one hand, ratifies that the Web enables access to

[141] Available on https://www.w3.org/1998/02/Potential.html Access on 17th June 2019.

information, and on the other hand it recognises that nowadays this is privately achieved through encryption and anonymity, both of which are provided by Tor.

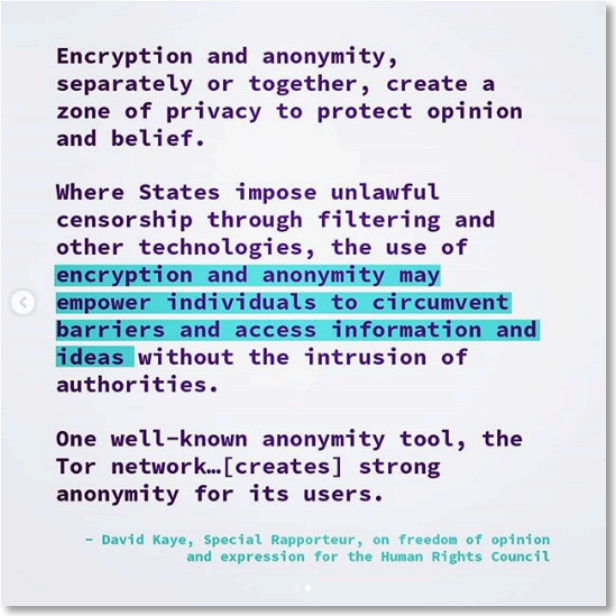


Figure 14: Post by The Tor Project: David Kaye (10th December 2018)
Source: The Tor Project Instagram account (@TorProject)
Retrieved by the author in May 2019

Although is not possible to say if these statements attract users and expand Tor's popularity, the fact is that the use of this technology is consistently growing. In 2018, the average number of daily users of the technology worldwide was equivalent to 2.39 million,[142] according to information provided by Tor Metrics, which provides data without encroaching on users' privacy[143]. In that year, there was a peak of 4.35 million people using Tor in 26th January 2018. Compared to the earliest available data, from 2011, when the number of average daily users of Tor worldwide was 658,593, there was growth of 362% between 2011 and 2018. In addition,

[142] Available on https://metrics.torproject.org/ Access on 22nd May 2019.
[143] More information about how Tor collects data from users assuring their privacy is available on https://metrics.torproject.org/about.html Access on 5th August 2019.

considering UK access only in 2018, the average number of daily users was 62,968, with a peak of 77,623 people on 28th January 2018.[144]

Taken also from Tor's Instagram account, the next posts are composed of personal statements that exemplify how the platform can be applied in everyday life for multiple justified purposes. The first example (Figure 15) is related to Tor being used by a political activist who defends freedom of speech and fears being targeted by authorities: '[B]eing a dissident is hard enough, privacy is already heavily curtailed, so anonymized communication is a godsend.' The second (Figure 16) is about a medical doctor protecting data belonging to high-profile patients. And the last example (Figure 17) shows a father who uses Tor for research-sensitive topics and is concerned about his children's personal issues and privacy.

[144] According to Tor Metrics, the relevant event that happened around these dates was the release of a latest and updated version of the browser, called Tor 7.5, on 24th January 2018, which could potentially have increased interest in the technology.

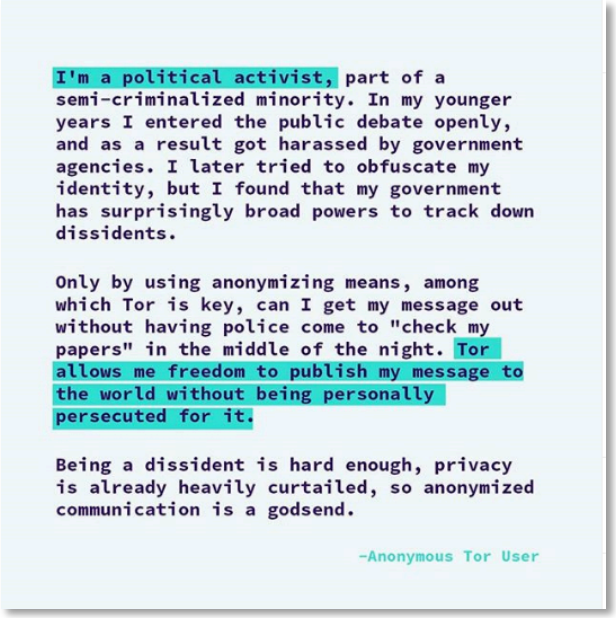


Figure 15: Post by The Tor Project: political activist (30th December 2018)
Source: The Tor Project Instagram account (@TorProject)
Retrieved by the author in May 2019

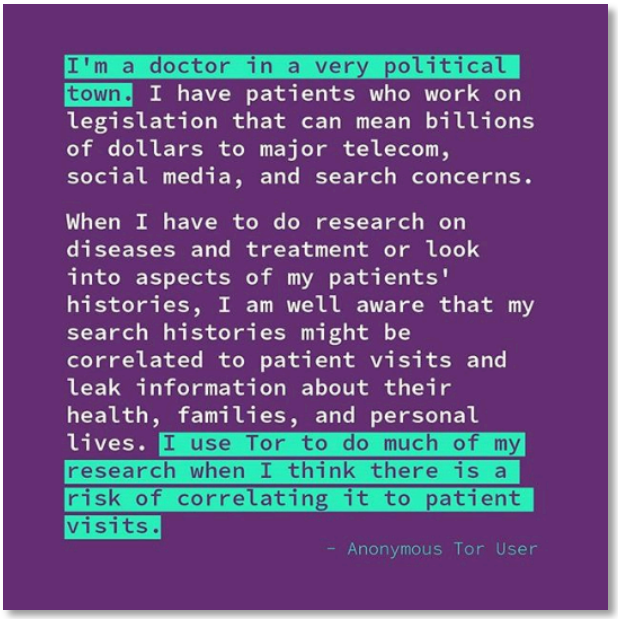


Figure 16: Post by The Tor Project: doctor (1st March 2019)
Source: The Tor Project Instagram account (@TorProject)
Retrieved by the author in May 2019

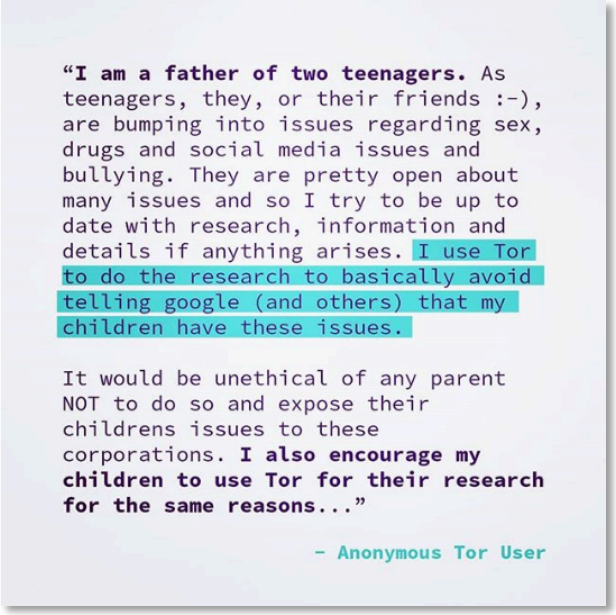


Figure 17: Post by The Tor Project: father (26th November 2018)
Source: The Tor Project Instagram account (@TorProject)
Retrieved by the author in May 2019

This brief review shows that The Tor Project presents itself overall in a completely positive way through online platforms such as websites and social media, without mentioning negative connotations. Furthermore, this tool is consistently portrayed as useful for protecting privacy for several purposes, as well as necessary to avoid surveillance by state and corporations. Moreover, Tor is celebrated for giving an alternative to people who need online anonymity for everyday tasks. In conclusion, its self-mediation is purely positive and ignores any negative connotations, albeit they do exist, as discovered in the discussion in the next chapter. The same can be seen in many other software and online services, such as Facebook and other social media, which present themselves through their advantages, not disadvantages. More balanced views of this tool are presented by scholars (McCoy et al., 2008; Hoang & Pishva, 2014; Jaeger, 2015; Sui et al., 2015; Jardine, 2018b), but this research focuses, at this point, on the extent to which British newspapers reproduce this positive discourse.

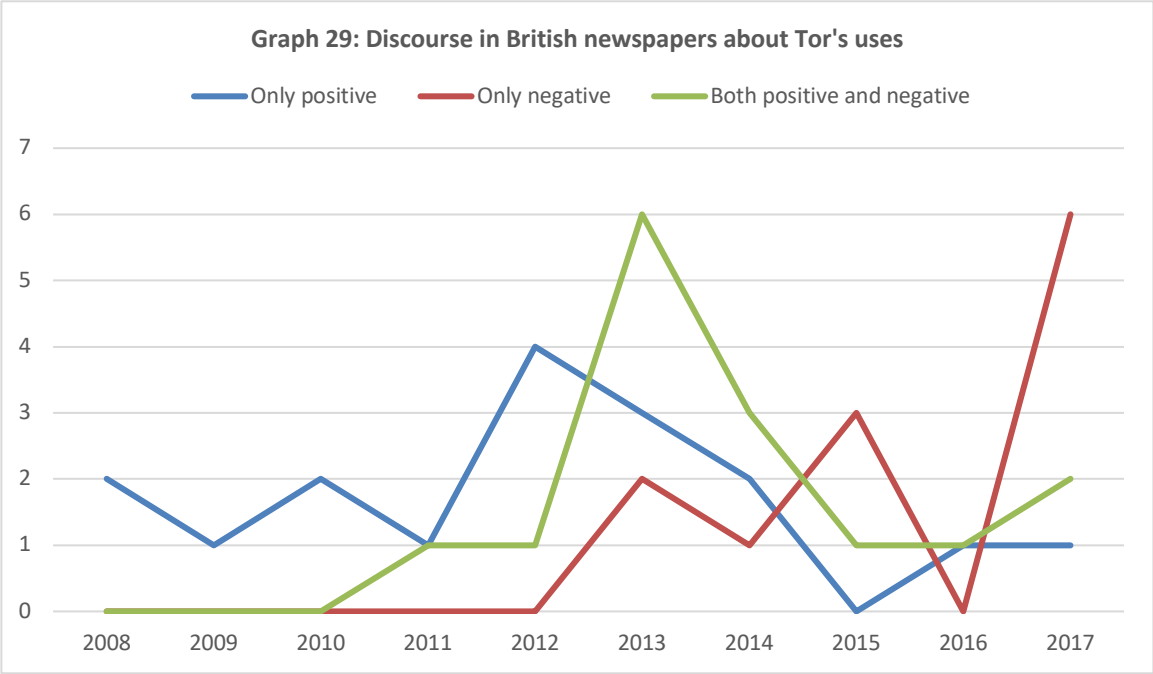
6.2 Liberation Discourse in the British press's Coverage of the Tor Network

It is safe to say that Tor's self-mediation through its website and social media adopts an entirely positive discourse by presenting this tool as a liberation technology that is mandatory if one wishes to achieve privacy on the Web. The last section made this clear, and this section now examines cases in which the same perspective is adopted by the British press. As a result, this research looks at examples of newspaper articles that explore only the positive outcomes of Tor and ignore the negative ones. Consequently, this section examines these articles by using critical discourse analysis, a method through which reality is not only described, but also evaluated and explained (Fairclough, 2004).

As argued in the Methodological Framework, 'CDA (*critical discourse analysis*) is about the underlying ideologies that play a role in the reproduction of or resistance against dominance or inequality,' a method that aims 'to uncover, reveal or disclose what is implicit, hidden or otherwise not immediately obvious in relations of discursively enacted dominance or their underlying ideologies' (van Dijk, 1995, p. 18). Thus, CDA is related to the examination of how dominance is expressed, and it is worth noting here that media discourse is connected to the elites, since 'patterns of discourse control and access are indeed closely associated with social power' (van Dijk, 1995, p. 20). According to van Dijk (1995), this control can be identified, for instance, when the media set the agenda, which can be seen extensively in the discussion presented in the previous chapter, showing Deep Web technologies constantly linked to criminal and antisocial behaviours.

The initial step in understanding the overall discourse of British newspapers about Tor requires identifying the selected approach to the topic, which involves looking into media messages and searching for 'meaning, interpretation and understanding' (van Dijk, 1995, p. 21). In order to achieve this aim, as explained in the *Methodological Framework*, this research analysed 58 articles mentioning Tor and published in six British newspapers, and it identified four approaches related to how it is portrayed over time. Coverage was considered positive when the article had an entirely optimist view of the technology's uses, for instance the protection of freedom of speech or the right to online privacy, and negative in the case of the opposite, with articles focusing only on criminal or antisocial connotations such as crypto markets. Both positive

and negative coverage occurred when the article presented the technology's ambivalence, and coverage was classed as ignored for cases in which there were no mentions of connotations or uses. After this initial analysis, 44 articles were identified as describing activities that this tool enables and are represented in Graph 29: 17 mention only positive uses, 15 articles present both positive and negative uses and 12 mention only negatives. The other articles ignored the reasons why Tor is used.



As Graph 1 shows, the overall discourse about Tor highlights positive uses up to 2012, but from that point onward the newspapers preferentially acknowledge both sides or only negative aspects. This variation can be explained by the association made between Tor and the crypto market Silk Road, which was shut down in 2013, increasing the number of articles relating the technology to criminal behaviours. Silk Road was developed to be accessed through Tor, and therefore both crypto market and technology are constantly linked by the media. This chapter, however, examines the 17 articles in which Tor is framed only as a positive. The other articles mentioning distinct uses of Tor are discussed in the next chapter.

Although this research includes content from six tabloid and quality newspapers, these 17 articles mentioning only optimistic views of Tor are distributed in only half of them: 13 published

in *The Guardian*, three in *The Times* and the remaining one in a tabloid newspaper, *The Sun*. In Table 14 (see below), it is possible to see the headlines used by newspapers in articles related to Tor, in chronological order. It is not a surprise that quality newspapers are more open to acknowledging the benefits of Tor as a liberation technology, since tabloids usually adopt a condemnatory discourse on the Deep Web and reproduce stereotypes related to crime. Cross (2014, p. 215) in this regard argues that 'tabloids are the main cultural arena that daily constructs stories of urban criminality.' It is not a surprise either that *The Guardian* acknowledges Tor's positive outcomes, since this newspaper was partly responsible for the Snowden revelations and openly criticises state surveillance, which is usually portrayed as 'immoral, unjustified and widespread' (Branum & Charteris-Black, 2015, p. 205).

Table 14: Headlines about positive uses of Tor in British newspapers

	NEWSPAPER	PUBLICATION	HEADLINE
Case 1	The Times	15th May 2008	"What else happened"
Case 2	The Guardian	7th August 2008	"Chaos aims to crack China's wall"
Case 3	The Times	29th December 2009	"The YouTube revolution: how a view from the barricades boosts protesters' cause"
Case 4	The Guardian	23rd March 2010	"Google in China: Inside the firewall, information is in short supply for web users"
Case 5	The Guardian	25th March 2010	"Chinese censorship: Tricks to beat the online censor"
Case 6	The Times	1st June 2011	"Judge to rule in 'Goodwin affair woman'"
Case 7	The Guardian	2nd March 2012	"Protecting yourself: delete, or block? How to avoid giving too much away"
Case 8	The Guardian	3rd April 2012	"UK's plan to track online traffic 'sanctions regime elsewhere'"

Case 9	The Guardian	20th April 2012	"Online identities: is it more important to have a single persona or the freedom of anonymity?"
Case 10	The Guardian	21st April 2012	"Hacktivism: the web's most influential people and groups"
Case 11	The Guardian	11th June 2013	"Prism break: is it really possible to exist online without casting a digital shadow?"
Case 12	The Guardian	24th June 2013	"Surveillance and the limits of GCHQs powers"
Case 13	The Sun	30th June 2013	"Beware the Big Brother with eye for bank secrets"
Case 14	The Guardian	11th March 2014	"Snowden: leaks have boosted US security"
Case 15	The Guardian	13th June 2014	"Wildlife WikiLeaks exposes major environment crimes"
Case 16	The Guardian	2nd November 2016	"Dark web departure: fake train tickets go in sale alongside AK-47s"
Case 17	The Guardian	4th August 2017	"Secret internet browsing histories put up for sale"

An overview of this table indicates topics that are usually present in discussions about Tor, such as privacy, surveillance, whistle-blowing and anonymity. Thus, in the next subsection, this research analyses those points through which Tor is addressed as a liberation technology by the British press. To find these common arguments, these 17 articles were examined by using critical discourse analysis according to Tor's news values, and therefore 'the "newsworthy" aspects of actors, happenings and issues as existing in and constructed through discourse' (Bednarek & Caple, 2014, p. 137). This research looks at ideas emphasised in the articles through the 'analysis of frequency (word forms, lemmas, clusters), analysis of keywords/clusters or grammatical/semantic tags, dispersion analysis, concordancing, etc.' (Bednarek & Caple, 2014, p. 141). The classification that follows is ensured in terms of the main topics addressed by the

newspapers, in an attempt to organise the analysis, but it does not mean that one article is exclusively about one topic and ignores others. Furthermore, an article examining state censorship will most likely mention privacy, while an article about activism will also talk about online anonymity and so on.

Fighting State Censorship and Surveillance: For Democracy and Freedom

One reason why Tor is so popular as a liberation technology is because it is constantly associated with the battle against censorship and surveillance perpetrated in multiple ways, especially by governments, across the world (Diamond, 2012). Furthermore, according to Tor's website, one of the main purposes of this technology is to avoid control: '[W]e, at the Tor Project, fight every day for everyone to have private access to an uncensored internet, and Tor has become the world's strongest tool for privacy and freedom online.'[145] Likewise, this association between using Tor and escaping surveillance practices is made by the British press: considering all 833 articles included in this research, content analysis shows that 31.6% of them mention surveillance practices, and 5.8% mention some sort of state censorship. Considering only the 58 articles that mention Tor, however, these numbers increase to 74.6% and 35.6%, respectively.

This analysis shows that there are cases in which newspapers – quality, in particular – criticise this practice, as seen in an article entitled "Dark web departure: fake train tickets go on sale alongside AK-47s,"[146] published by *The Guardian* in November 2016. As the extract below shows, although this article addresses criminal activities in crypto markets, it offers a differentiation between negative uses of the Dark Web and the Tor Network, a distinction which is not that common in the British press (as seen in Chapter 4).

```
1 These marketplaces make up a fraction of what constitutes the dark web, which
2 operates in parallel to the traditional web and typically requires invitation
3 or special authorisation to access. Up to 30,000 dark websites were estimated
4 to exist in analysis done last year, Dr Lee says. "Only 50 were marketplaces.
5 The rest could be file-sharing or private forums, for example." Other parts of
```

[145] Available on https://www.torproject.org/about/history/ Access: August 2019.
[146] Related article: "Dark web departure: fake train tickets go on sale alongside AK-47s," The Guardian, 2nd November 2016, Technology, page 3.

```
6 | the dark web, including Tor, operate as benign lifelines for citizens in
7 | authoritarian states.
```

An item that requires special attention is the highlighted sentence in the extract above (lines 6 and 7), because more than portray this technology in a positive way, this article encourages its use, citing authoritarianism as a motivation. Furthermore, and still according to this article, using Tor is a response to governmental abuse, a requirement in view of the current amount of state censorship. The article also attributes to Tor a brave role, using the expression 'benign lifelines' to define its activity, which denotates that Tor is virtuous as well as directly responsible for protecting and saving people's lives. Finally, the use of the word "citizens" to define Tor users also shows a choice to highlight the political aspect of this technology. According to Cooper (1991, p. 5), this term relates to the individual and the community, since 'this status and role may be formally codified in terms of qualifications, rights, and obligations by constitutions, charters and laws, or informally determined by values, tradition and consensus.'

In the below extract, also published by *The Guardian*, the same topic was raised by a member of the public in a letter entitled "Surveillance and the limits of GCHQs powers"[147]:

```
1 | I'm getting rather tired of all this hand-wringing about the NSA and GCHQ (and
2 | other members of the "five eyes") intercepting our communications. In 2001 a
3 | committee of the European parliament published a substantial report
4 | (goo.gl/gSNpS) on the Echelon system, and recommended that we all encrypt our
5 | emails using, for example, an OpenPGP system such as GnuPG (GPG, free) or PGP
6 | (commercial). Anyone who followed that advice has nothing to worry about when
7 | it comes to interception of email content. This does not address the metadata
8 | problem, in particular traffic analysis: to deal with that you need to use a
9 | Tor system, which is rather more complex to set up.
```

The letter reproduced in the extract above was written by Doctor Alun J. Carr, based at the School of Mechanical and Materials Engineering at the University College Dublin. First of all, the writer has technical knowledge on the topic, which is not necessarily the case for the majority of

[147] Related article: "Surveillance and the limits of GCHQs powers," The Guardian, 24th June 2013, Leader Pages, page 27.

the public. From the outset, Doctor Carr uses the expression 'I'm getting rather tired' (line 1), which in this context demonstrates a condescending reaction to other people's concerns about surveillance as well as a feeling of superiority related to people having a supposedly late reaction to these issues. Thereafter, the text cites an official report (lines 2 to 6) providing recommendations on how to ensure encrypted mail as if they were obvious to everyone – although they require a level of interest in the topic as well as an understanding of technology.

Finally, the same extract presents a patronising comment, not only ironising people's issues, but also suggesting that those to blame for surveillance are those who do not use appropriate protective measurements: '[A]nyone who followed that advice has nothing to worry about when it comes to interception of email content' (lines 6 and 7). At the end, Doctor Carr mentions Tor as a viable and complex way of protecting communications from traffic analysis and suggests its use. This extract presents a point of view of someone that has experience with technology, which in this case is adopted and accepted (Rama Murthy & Mani, 2013), and this reflects in the person's ideas and actions. For the author, the use of Tor should be obvious. Although the message could be more educational and less judgmental, the overall argument is that Tor is an evident protection against surveillance. There is no objective disapproval, however, levelled at why surveillance is so well-established, i.e. through government actions.

A case of direct criticism of surveillance practices in the United Kingdom is evident in an article by *The Guardian* entitled "UK's plan to track online traffic 'sanctions regimes elsewhere'"[148] and published in April 2012 (see the extract below). In this case, Tor is introduced in a positive way as a 'shield' (line 1) and therefore a device used for protection. Although the use of Tor is initially connected to activists resisting authoritarian regimes abroad (lines 1 and 2), this article overall presents surveillance as it happens in the United Kingdom as a reason why people should use this technology (lines 2 and 3). Additionally, it includes a relevant question proposed by a member of The Tor Project about data (lines 6 to 7), promoting a necessary discussion about how governments deal with private information and what uses can be made of it.

[148] Related article: "UK's plan to track online traffic 'sanctions regime elsewhere,'" The Guardian, 3rd April 2012, Home Pages, page 6.

```
1 The makers of Tor, the internet anonymity shield used by activists in Iran and
2 China, said that it would support users who wished to evade detection by UK
3 authorities. Andrew Lewman, the director of Tor, compared the UK plan to the
4 data retention laws in Germany that require internet providers to log users'
5 website visits. He said use of Tor rose after that law was introduced. "Once
6 the data is collected, regardless of the current intentions, it will be used
7 for all sorts of reasons over time," Lewman told the Guardian.
```

Generally, the British media condemn governmental practices of censorship and surveillance, albeit this approach applies more stringently when discussing foreign governments. Furthermore, this analysis shows that *The Guardian* pays special attention to the situation in China, with three articles on the topic. Previous research about *The Guardian*'s coverage of freedom of speech affairs shows that this newspaper overall defends digital media as giving power to the people so they can control more closely authorities' actions as well as organise themselves against government misconduct (Imre, Pjesivac & Luther, 2016). In addition, surveillance issues in China are a topic afforded special attention, due to the 'censorship's cultural logic' (Yang, 2016, p. 1377) in a context of economic relevance, as China has the second-largest economy in the world and is home to the greatest population.

The first article on the topic is entitled "Chaos aims to crack China's wall,"[149] published in August 2008, about how journalists planned to deal with Chinese restrictions on the Internet during the Beijing Olympic Games that year. First, the article begins with a paragraph (lines 1 to 5) that directly mentions censorship twice and instigates a response while saying that hackers are fighting against the Chinese state. The use of the expression 'your help' while addressing the reader makes an immediate connection between the reader and the argument, a strategy to instigate support while defending a point (Bednarek & Caple, 2014). In addition, the use of the word 'help' on line 5 determines a need for action.

```
1 It was John Gilmore, founder of the Electronic Frontier Foundation,
2 that the internet interprets censorship as damage and routes around it. For
3 years, the Chinese authorities have done their best to prove him wrong. Now,
```

[149] Related article: "Chaos aims to crack China's wall," The Guardian, 7th August 2008, Technology Pages, page 1.

```
4 with the Beijing Olympics upon us, a group of hackers has launched an attempt
5 who said to stamp out censorship there - and they want your help to do it.
```

Through the text, this article also criticises Chinese restrictions to Web access, calling it 'censored' and 'filtered,' framing it as 'problematic' and comparing it to the idea of open access:

```
1  The Chinese authorities have censored access to western sites from within the
2  country for years, but in the run-up to the games, the issue has become
3  increasingly problematic - and public. The authorities have been sputtering
4  towards the idea of an open internet, first declaring that journalists could
5  access previously filtered western sites, and then reneging on the idea at the
6  11th hour. According to the Open Net Initiative (opennet.net), which monitors
7  state surveillance and filtering online, the Chinese government has now opened
8  access for the media to many sites, but it is still using techniques to stop
9  access to sites when users search on certain keywords. What is not clear is
10 whether everyone in China has access to the sites that have been opened, nor
11 whether they will remain available after the games are over.
12 CCC's downloadable toolkit contains software that provides access to Tor, a
13 network of computers designed to make internet traffic anonymous. Tor consists
14 of volunteer computers that relay traffic between each other without knowing
15 its ultimate source or destination. It makes it difficult for observers to
16 track where internet traffic is going, or who sent it.
17 Tor isn't new. It was originally based on technology developed by the US navy.
18 But it is appropriate for the job, says Fred von Lohmann of the Electronic
19 Frontier Foundation, which sponsored the development of the network until 2005.
20 "Tor lets you see what the world looks like from someone else's net
21 connection," he says.
```

The background offered by the author of this piece helps to construct a picture of what is involved in restricted Internet access in China, following which Tor is introduced as a solution (lines 12 and 17), which is made mainly by opposing online anonymity to tracking. Finally, the last paragraph (lines 17 to 21) presents other positive understandings of this technology. According to a member of the Electronic Frontier Foundation, 'Tor lets you see what the world looks like from someone else's net connection' (lines 20 and 21). Therefore, this technology is associated with idealised usage, allowing users the experience of being free on the Web, seeing the world

with no restrictions and accessing knowledge and information around the globe. It is an optimistic defence of this technology that would make Negroponte proud.

Chinese censorship is raised again by *The Guardian* in March 2010, in the article "Google in China: Inside the firewall, information is in short supply for web users,"[150] which also addresses state control in a critical and concerned manner. As the extract below shows, this article mentions disapprovingly the role of the Chinese government in actively controlling Internet access, using words such 'zeal' and 'blocked' (lines 3 and 5, respectively). In addition, the provided definition of Tor (lines 3 and 4) presents a positive slant on its role, highlighting the anonymity this tool enables and linking it to the idea of helping users (line 3), especially in the context of condemning state surveillance.

```
1 But Dr Steven Murdoch, a researcher at the computer laboratory of Cambridge
2 University, said Chinese authorities have been using such methods with
3 increasing zeal. Murdoch is a member of the Tor project, which helps internet
4 users surf the web anonymously, and says that the IP addresses it uses are
5 blocked as quickly as the authorities can find them.
```

Entitled "Chinese censorship: Tricks to beat the online censor,"[151] a third article published by *The Guardian* on the topic shows again strong views against the practice. The article offers a direct positive perspective of privacy-enhancing technologies, suggesting that people should use Tor to escape state surveillance in China with a provocative discourse that does not hide its bias (see the previously mentioned title). Although the paragraph including Tor in the list of tools against surveillance is brief, it fills an educational role by providing an explanation about how this works, as well as how encryption can help users looking for privacy:

```
1 Tor (The Onion Router) sets up a proxy server on the user's computer then sends
2 encrypted signals to other Tor routers around the web. To the censors, it looks
3 like more encrypted traffic.
```

[150] Related article: "Google in China: Inside the firewall, information is in short supply for web users," The Guardian, 23rd March 2010, Home Pages, page 6.
[151] Related article: "Chinese censorship: Tricks to beat the online censor," The Guardian, 25th March 2010, International Pages, page 25.

This overall condemnation related to censorship is not exclusive to *The Guardian*, and China is also not the only target. An article in *The Times*, for instance, discusses the use of Tor to protect freedom of speech and information in the context of the Middle East:[152]

```
1  News is pouring out despite the best efforts of the Iranian censors. The
2  monitoring centre is believed to engage in a process called Deep Packet
3  Inspection, which deconstructs every packet of digitised data, examines it for
4  keywords such as "democracy" and "freedom" and then reconstructs it within
5  seconds. This enables the Government to monitor protesters' activities, block
6  communications and gather information. But in this continuing cat-and-mouse
7  game the opposition is winning. Many are using proxy servers to connect to the
8  internet and either e-mail or upload their films. Proxy servers are servers
9  that act as intermediaries for internet users seeking to access banned sites.
10 For example, TOR - The Onion Router - bounces users' requests through a chain
11 of routers around the world, rather like a cybercell system where no single
12 router knows the complete data path. "Citizen journalists in Iran are
13 technically very savvy. They send their films and pictures out to their
14 contacts, who upload the material for them. The internet is hugely important in
15 getting information out of Iran and for people in smaller cities there to know
16 what is happening," said Golnaz Esfandiari, an Iranian-born journalist for
17 Radio Free Europe/Radio Liberty, based in Prague.
```

This extract offers some background information on how surveillance practices are conducted in everyday life in Iran (lines 1 to 6), which contributes to understanding the extent of the issue. In this case, it is related to how Iranian authorities are actively using technology to track political activists researching "democracy" and "freedom" on the Web. This scenario makes an emotional appeal, because it instigates division between wrong and right, namely authoritarianism imposing limitations vs. people fighting for democracy and freedom. This article also presents a set of alternatives to challenge the situation (lines 7 to 12), with the Tor Network being one such choice. When Tor is included as an option to fight state censorship, as a resource in the battle against surveillance, it embraces the ideals of a liberation technology which helps

[152] Related article: "The YouTube revolution: how a view from the barricades boosts protesters' cause," The Times, 29th December 2009, News, page 6.

people achieve online freedom. In addition, this article addresses the discussion on the digital literacy required to use Tor: the term 'technically very savvy' (line 13) is mentioned by a source to define people that can use these tools and protect themselves.

Another article from *The Guardian* provides a discussion about surveillance in the context of the United States, with the title "Snowden: leaks have boosted US security:"[153]

```
1  James Clapper, the director of national intelligence, has admitted not telling
2  the truth when he told a congressional hearing last year that the government
3  was not "collecting data on millions of Americans." Snowden said Clapper had
4  shown officials "can lie to the country, lie to the Congress, and face not even
5  a criticism." He encouraged ordinary internet users to protect themselves
6  against surveillance by encrypting both their hard drives and their online
7  activity, describing encryption as "the defence against the dark arts in the
8  digital realm." He also advised people to browse the web anonymously using the
9  Tor system. He urged software developers to create more user-friendly secure
10 communications tools that could "pass the Glenn Greenwald test," referring to
11 Greenwald's inability to communicate securely using PGP encryption when Snowden
12 first approached the journalist, then working for the Guardian. However he
13 warned: "If you are a target of the NSA, it is game over no matter what unless
14 you are taking really technical steps to protect yourself."
```

In this article, as the extract above shows, there is clear opposition between governmental and people's interests when discussing Snowden's leaks. Initially, it presents a member of the United States government caught in a lie to not only create awareness of surveillance practices and data collection (lines 1 to 3), but also to state that the government cannot be trusted (lines 3 to 5). In the next moment, it presents a solution to the matter via Tor and portrays encryption as a defence instrument (lines 5 to 9). The article also addresses the issue of digital literacy, including a claim made by Snowden regarding the development of new technologies that can help regular users protect themselves against state surveillance (lines 9 to 12). The same claim is made for Diamond (2012), for whom countries with more resources should invest in these technologies and assure they are accessible to everyone. The same article, however, explains

[153] Related article: "Snowden: leaks have boosted US security," The Guardian, 11th March 2014, Home Pages, Page 3.

that if a regular Internet user is targeted by authorities and the person lacks technical knowledge, then there is no solution – Snowden directly uses the term 'game over' (line 13).

Overall, newspapers' discourse on the topic of surveillance is heavier in criticism when abuses happen abroad. Collins et al. (2011, p. 15) support this notion, claiming that 'the British media is more competitive and aggressive in its international coverage.' From the seven cases analysed in this section, only one directly mentions a British agency as the source of surveillance practices, with the others citing examples from China, Iran and United States, or discussing generically the fight against authoritarian regimes. Although extreme cases are indeed prevalent in undemocratic states, democratic societies are also subject to distinct levels of surveillance (Diamond, 2012), but British newspapers dedicate more attention and analysis to the way surveillance happens overseas.

Protecting Privacy: Re-Thinking Mass Surveillance

Privacy is another recurring topic among articles discussing Tor. Considering the 833 articles used in this research content analysis, 41.4% mention privacy issues, but in the case of articles citing Tor, this number goes up to 79.7%. This subsection addresses examples in the British newspapers in which privacy is the motivation for using Tor as a liberation technology, and it starts with an example from the tabloid newspaper *The Sun*. An article published in June 2013 and entitled "Beware the Big Brother with eye for bank secrets"[154] presents an interesting overview of Snowden's revelations, even citing "Big Brother" and "George Orwell" to explain the constant surveillance to which societies are submitted. Instigating a broader discussion, this article refers to surveillance tools such as Prism (line 1) in a disapproving way with the term 'prying project' (line 2), which means "nosy." In addition, this article clarifies that surveillance practices are not exclusive to authoritarian regimes:

```
1 When CIA man Edward Snowden blew the whistle on Prism - America's secret web
2 prying project - it forced us to re-think the idea that "free" nations don't go
3 in for mass surveillance.
```

[154] Related article: "Beware the Big Brother with eye for bank secrets," The Sun, 30th June 2013, Features, page 34.

The overall focus of the article is to raise awareness of the constitutional right to privacy in the United Kingdom. Therefore, it helps exemplify how the British press portray Tor as a liberation technology related to the domestic, not the foreign, context. With an educative approach, this article provides a list of measurements that can be taken to protect personal data from traffic analysis, including Tor:

```
1 Another good protection method is to ensure you don't leave any trace of your
2 online history. Most web browsers now offer an "anonymous" or "private"
3 browsing mode which scrubs any record of site visit "cookies," as well as
4 details of your searches and web-form entries. There are highly anonymous
5 browsing services like Tor which promise to defend you against web surveillance
6 but using them will probably flag you to the Prism spooks! Anti-spyware
7 and registry cleaning software will also help ensure that sneaky data mining
8 programs don't get on to your computer.
```

This article presents Tor as one of a number of 'good protection' methods (line 1), which means that it acknowledges not only the existence of a problem – in this case, surveillance –, but also that the problem requires protective measurements. The article then fills an educational role by raising awareness of privacy issues, explaining multiple ways in which people can protect themselves from traffic analysis and, fundamentally, opening up this relevant discussion. The same extract mentions that the government's power cannot be underestimated, however, because even using protective measurements can be considered by authorities to be a suspicious online behaviour (line 6). Overall, this article presents a condemning discourse directed at surveillance practices, as exemplified through the use of the disapproving term 'sneaky' (line 7), meaning 'furtive,' to refer to data-mining programs used by governments.

Another example is the article "Protecting yourself: delete, or block? How to avoid giving too much away,"[155] published by *The Guardian* in March 2012. This article looks at ways that private companies such as Google collect personal information and presents tips on how to block

[155] Related article: "Protecting yourself: delete, or block? How to avoid giving too much away," The Guardian, 2nd March 2012, Home Pages, page 19.

tracking services and activate private browsing to avoid tracking. Among other forms of keeping data private, this article mentions anonymous browsing sites:

```
Websites identify the IP (internet protocol) address you use to access the web.
So, instead of going directly to a website, go via one or more intermediate
websites, or proxies, so it can't see where you started. Various "anonymous
proxy" websites - some free, some commercial - make this simple. Examples
include hidemyass.com, anonymouse.org, Proxify and Megaproxy. The most
comprehensive anonymous browsing service is the peer-to-peer Tor (The onion
router) network. However, free proxy services tend to be slow, will not access
certain sites, will not download large files, and have other measures to
prevent abuse.
```

The above extract shows that Tor is not only cited as an option among privacy-granting technologies, but it is mentioned as the most relevant choice. Therefore, the network is represented as a way of achieving a safe connection, as would be expected from a liberation technology. Finally, the article also provides drastic advice:

```
If you can avoid social networks altogether, that should also increase your
privacy.
```

This sentence instigates a timely discussion about alternatives to using the Web privately, and if they are sufficient. This distrust of the system also appears in an article published by *The Times* in August 2017 and entitled "Secret internet browsing histories put up for sale,"[156] which discusses to what extent Web-browsing histories are private when users activate modes that should increase data protection. In this instance, the "Incognito mode" in the Google Chrome browser is discussed:

```
Browser extensions are turned off by default in Google Chrome's incognito mode,
but the researchers warned that even if this setting were used internet service
providers still retained records that could be at risk of being compromised.
```

[156] Related article: "Secret internet browsing histories put up for sale," The Times, 4th August 2017, News, page 11.

```
They discovered a politician who had searched for a herbal supplement to
stimulate an ageing brain and a judge who browsed porn sites. Although the
identities of the individuals in the German database were supposedly protected,
the researchers were easily able to work out who they were using a method
devised nine years ago. Speaking at a hacking conference in Las Vegas, they
said that the only way to keep browsing histories truly private was to use a
virtual proxy network or the browser Tor.
```

As the extract above points out, modes available on mainstream browsers are not a guarantee of avoiding data collection or keeping histories private – assumptions that could easily be made by users with less experience of using the Web. If the answer is not to use the resources offered by these browsers, then the article mentions an effective way of protecting private data: using VPNs or Tor (lines 9 and 10). Another point to discuss from this article is the alarming information provided by a data broker to the researchers while they were negotiating browsing histories:

```
The researchers were repeatedly told that it was easier to obtain data for UK
and US residents than for Germans.
```

There is notable emphasis on the word 'repeatedly,' which means someone making the same point over and over again. In this case, the point is that it is easier to buy private data about the browsing habits of British and North American people than it is for Germans. There is no explanation in the article if surveillance issues are more severe in the United Kingdom and the United States, or if users from these two countries are careless with personal data when compared to the Germans. According to the results of a comparative study on the topic of covert surveillance, however, Germany presents 'perhaps the most sustained and self-conscious effort to control and legitimate undercover policing' as well as 'higher-order values, including fundamental rights like privacy' (Ross, 2007, p. 496).

Another example of a positive view of Tor used as the main argument for the right to privacy, an article published by *The Guardian* in June 2013 and entitled "Prism break: is it really possible

to exist online without casting a digital shadow?"[157] presents the following introduction to the topic of the Snowden leaks:

```
1 Consumers worried about their internet privacy in the wake of the online
2 snooping revelations have the option of using some alternatives to the likes of
3 Google and can try to use more secure forms of communication - if, that is,
4 individuals believe maintaining their online security is worth it.
```

This extract disapproves of surveillance practices, evident in its use of the term 'snooping' (line 2), which is associated with furtive action, by listing Google as an unsafe form of communication (line 3) and suggesting the adoption of protective measures (line 3). Additionally, the final sentence of the paragraph (lines 3 and 4) uses irony to reinforce that everyone should consider that online security is something worth pursuing and maintaining. To this introduction is added a list of elements to consider related to security and privacy. The mention of Tor is a reply to the question, "How can I anonymise my online activity?":

```
1 The more heavyweight option is to mask your IP address, the unique
2 identification number of every device that connects to the internet, and there
3 are three main choices: The Onion Router
4 (http://www.Torproject.org/projects/Torbrowser.html.en), or TOR, is free and
5 will disguise your IP address, but can be complex to set up.
6 Another option is to use a different server or proxy, which can be done by
7 changing individual access settings on your machine. The third option is to
8 subscribe to a VPN service.
```

The article includes Tor not just as an option to achieve online anonymity, but also as one of the best alternatives available, as seen in the use of the expression 'more heavyweight' (line 1). Adding to this point, the use of the word 'free' (line 4) to define this technology can help to instigate its adoption, because the download does not require payment, which may potentially make it more attractive. Finally, the article also mentions that Tor is 'complex' (line 5),

[157] Related article: "Prism break: is it really possible to exist online without casting a digital shadow?," The Guardian, 11th June 2013, Home Pages, page 7.

information that prepares prospective users for the technical challenges of installing and adopting Tor in everyday life. This example, as well as the previous ones presented in this item, shows that positive views of Tor in British newspapers argue in general about this technology as a viable option to achieve privacy and as a response to surveillance practices, thereby instigating its use as a form of emancipation, without ignoring that it requires a level of comprehension.

Assuring Online Anonymity: The Hope to Re-Anonymise the Web

A fundamental part of online privacy is directly connected to anonymity, the achievement of which is the main purpose of Tor. Miller (2011, p. 113) argues that anonymity is 'a peculiarly modern element of privacy. People are seen to be deserving of the right of protection from unwanted attention and scrutiny, or the right to simply be "a face in the crowd" and go about one's business unhindered by the surveillance or attention of others.' Considering that the liberation technology discourse is related to examining ways in which freedom can be enabled for political, social or other purposes (Diamond, 2012), this rhetoric is seen in articles published by British newspapers framing online anonymity as a general right. This research demonstrates that the media recognise anonymity as a central part of Tor and constantly associate one with the other. Furthermore, newspaper articles discussing Tor mention privacy in 74.6% of the cases, while articles about Deep Web technologies in general only mention privacy 28.7% of the time.

A case in which Tor is described in a positive way during a discussion about online anonymity can be found in an article published by *The Guardian* in April 2012 and entitled "Online identities: is it more important to have a single persona or the freedom of anonymity?"[158] This commentary presents, as the extract below shows, a very relevant debate about the end of online anonymity being motivated by corporations requiring an authentic identity, in the case of Facebook for instance, meaning that every person should have one account only, and multiple accounts are seen as some sort of fraud. The topic is directly addressed in the introduction:

```
1 | Before Facebook and Google became the megaliths of the web, the most famous
```

[158] Related article: "Online identities: is it more important to have a single persona or the freedom of anonymity?"[158], The Guardian, 20th April 2012, Home Pages, page 19.

```
online adage was, "on the internet, no one knows you're a dog.” It seems the
days when people were allowed to be dogs is coming to a close. The old web, a
place where identity could remain separate from real life, is rapidly
disappearing.
```

At the beginning of the extract above, Internet corporations are called ‘megaliths’ (line 1), which denotates an inflexible and large structure and shows a critical approach to the idea that Google and Facebook control the Web. In addition, a feeling of nostalgia can be identified in the use of the expression ‘old web’ (line 3), which is connected to the idea that people could hide their identities in the past (line 4). Thereafter, this article presents Tor as an alternative against these corporations’ logic. The extract below presents a member of the Tor Project as a source and reproduces the official argument of the initiative to encourage the use of the technology, which relies on the right to anonymity. This source defends the idea of ‘re-anonymis[ing] the web’ (lines 1 and 2), which in this context means giving back to people the right to choose if they want to be anonymous, or not. Moreover, as Lewman argues, the reasons for adopting Tor are connected to personal freedom and control, since people do not need to be identifiable all the time:

```
Andrew Lewman, executive director of the Tor Project, hopes to re-anonymise the
web. "The ability to be anonymous is increasingly important because it gives
people control, it lets them be creative, it lets them figure out their
identity and explore what they want to do," he says.
The Tor browser and software obfuscates a user's web traffic so anyone watching
is unable to trace who a user is or where they are coming from. This is a
technological solution to what Lewman feels is an elemental problem. "The
ability to forget, to start over is important," he argues. "Maybe you just got
divorced, maybe you just came out of rehab and you want to start over."
```

According to this article, the argument behind Google and Facebook’s option to impose the use of a single persona instead of allowing multiple accounts from the same person is purely commercial, since it is easier to collect personal data and use them to target adverts if a user has only one account. This is addressed ironically by the article, especially in the last paragraph:

```
1 And if they are successful at promoting their particular brand of authentic
2 identity, if you want to be a dog on the internet in the future, you'll have to
3 have papers to prove it.
```

Another example in which Tor is portrayed in a positive way in terms of anonymity is found in an article entitled "Hacktivism: the web's most influential people and groups,"[159] published by *The Guardian* in April 2012. The headline is self-explanatory, and the fact that this article includes Jacob Appelbaum, who is a Tor Project developer, as one of the most prominent people in his field shows the respect to this initiative's work. While describing Appelbaum, the article affirms:

```
1 Appelbaum is one of the core team of the Tor project, which protects the
2 anonymity of thousands of internet users across the world.
```

This brief but effective extract uses a specific verb to describe Tor's activity: '[protect]' (line 1). This means that Tor is seen not only as a relevant technology, but also as essential in defending people. In addition, the fact that the article mentions the impact of Tor 'across the world' (line 2), and not only in certain regimes, shows that the need for online anonymity is not limited to one or another political situation but is widespread throughout democratic and undemocratic nations.

In the extract below, there is a last example of anonymity highlighted by the British press: the article "Judge to rule on 'Goodwin affair woman,'"[160] published in June 2011 in *The Times*:

```
1 To avoid being identified, microbloggers are believed to be using software that
2 ensures online anonymity. Software, such as Tor, says that it routes internet
3 traffic through a worldwide volunteer network of servers that conceals a user's
4 location.
```

This item mentions Tor enabling Twitter users to apply online anonymity to discuss the extramarital affair of a public figure. The anonymity provided by Tor renders Twitter users

[159] Related article: "Hacktivism: the web's most influential people and groups," The Guardian, 21st April 2012, Home Pages, page 24.
[160] Related article: "Judge to rule on 'Goodwin affair woman,'" The Times, 1st June 2011, News, page 9.

unidentifiable while criticising politicians and claiming accountability. According to McLeod (2011), the use of online anonymity for discussing sensitive topics is one of the most reasonable applications, and therefore, by providing anonymity for these cases, Tor fills a relevant role in society.

Defending Whistle-blowing: "Maybe Onions are the Answer"

Controversially, as discussed before in this thesis, the activity of whistle-blowing has polarised opinion (Near & Miceli, 1996), as exemplified by the dichotomic reactions to Snowden's revelations about surveillance practices at the National Security Agency (NSA). While part of the public agrees that Snowden acted in the right way for exposing illegal and unethical practices, others see as antipatriotic and criminal the fact that he made public confidential documents with sensitive information about how the government agency works. According to The Tor Project, this case changed people's perspective on the topic: 'the need for tools safeguarding against mass surveillance became a mainstream concern thanks to the Snowden revelations in 2013. Not only was Tor instrumental to Snowden's whistleblowing, but content of the documents also upheld assurances that, at that time, Tor could not be cracked.'[161]

Since this is one of the most famous instances of whistle-blowing to date, and Tor was used in communications between the source and journalists, it is natural that there is an association between whistle-blowing and this technology. The same can be said about WikiLeaks, which was at the centre of Snowden revelations. Furthermore, WikiLeaks promotes itself, through its webpage, as specialising 'in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption,' and suggests people download Tor and submit documents through this platform.

In addition, the link between Tor and whistle-blowing is present in the media; in fact, it occurs in 18.6% of the articles about technology. In rare situations, as this section discusses, this connection is seen from a positive perspective. Curiously, the topic of whistle-blowing motivated

[161] Available on https://www.torproject.org/about/history/ Access: August 2019.

the publication of the first article about Tor among the researched newspapers, in *The Times*[162] in May 2008:

```
1 Would-be whistleblowers in Britain can face an uphill battle because only 40
2 per cent of businesses have measures in place to support them, says a report
3 from Grant Thornton, an accountancy firm. Maybe onions are the answer. The
4 Onion Router is a network that allows employees to post sensitive documents on
5 sites such as wikileaks.org without disclosing their internet address, New
6 Scientist (May 10) reports.
```

According to this article, Tor and WikiLeaks (line 5) are options for pursuing accountability among British companies – and this happened at least five year before Snowden made public documents proving unauthorised global surveillance. More than encouraging the report of misconduct, the article concentrates on the safety of whistle-blowers, directing clear criticism towards corporations that do not offer a secure option for people to report irregularities (lines 1 to 2). In this context, Tor (lines 3 to 6) is shown as an instrument of empowerment, since it establishes a safe option for employees to act against their employers. Therefore, Tor is the liberation technology necessary to create a controlled environment in which people feel able to highlight the misconduct of theirs bosses and share sensitive content of public interest. Overall, the combination of Tor and WikiLeaks, according to the article, improves accountability not only in the context of the industry, but also in the public sector.

WikiLeaks is mentioned again in another example, an article entitled "Wildlife WikiLeaks exposes major environment crimes" published in June 2014 in *The Guardian*. As the extract below shows, the use of the term 'WikiLeaks-style' (line 1) is related to websites that use Tor to enable the activity of whistle-blowing, allowing people to report wrongdoings and share sensitive information. In this case, the information is specifically related to environmental crimes, in that the main argument explains how providing a safe channel through which people can report crimes against nature is actively contributing to worldwide conservation.

```
1 A new WikiLeaks-style website targeting the kingpins of wildlife crime has
```

[162] Related article: "What else happened," The Times, 15th May 2008, Features, page 2.

```
attracted serious leads on elephant, tiger, fishery and forest destruction
across the globe in its first three months.
The WildLeaks website, which uses Tor technology to ensure anonymity, has been
set up by Andrea Crosta, an Italian security consultant who first revealed how
the al-Shabaab terrorist group in Somalia generated funds via ivory smuggling.
```

Furthermore, the extract below shows that this website's aim, namely protecting people's identity when reporting environmental offences, is seen as a possible answer against a state of 'pervasive corruption' (line 3), characterised by immoral authorities which allow these crimes to happen. Therefore, the website works not only for the direct protection of the nature, but also to assure that people are able to speak out against crimes, even when these violations are ignored by authorities that should otherwise be chasing criminals. Finally, a source connected to WildLeaks affirms that the tool is proving itself useful and necessary (lines 1 and 2), exceeding initial expectations and protecting lives.

```
"We had our first tip within 24 hours and the response has been beyond our
wildest imagination," said Crosta, now executive director of the Elephant
Action League. He said pervasive corruption meant whistleblowers frequently
feared that contacting local law enforcement could put their lives in danger.
"You can't, for example, export containers full of ivory from Mombasa without
bribing people left, right and centre," Crosta told the Guardian. "We
definitely feel we are filling a gap."
```

These examples, as well as the previous items in this section, through 17 articles portraying Tor optimistically in terms of its possible uses, illustrate that the British press can attribute to Tor a role of empowerment and protection against governmental or corporative abuses, a discourse in which it is in fact seen as a liberation technology. The reasons behind the use of Tor are diverse and according to geographical location, political situation, social aspects and other factors; in some cases, the issue is a radical state's surveillance, in others protecting the environment and so on. But overall the discourse in newspapers can present Tor as a tool able to offer an indispensable option for people in vulnerable situations. Thus, ultimately, British newspapers can acknowledge the need and the existence of liberation technologies that make people free on the Web.

6.3 Discussion: A Fearful Fight

Whilst presenting Tor through a constructive lens, albeit with a limited amount of examples, the British press recognise this technology's legitimate uses beyond criminal and antisocial associations. Actually, it makes sense that these newspapers discuss and in some cases openly defend Tor as a liberation technology. Tor is broadly seen as a response to surveillance and censorship practices, and so supporting its use also involves supporting freedom of speech, open access to knowledge, democracy and human dignity (Bellare & Rogaway, 2005; Cammaerts, 2013; Dingledine et al., 2004; Grey, 2016; Loesing, 2009; Moore & Rid, 2016), all values that should be protect by the media.[163] The Burmese journalist Win Tin even states, on the Reporters Without Borders website, that 'freedom of information is the freedom that allows you to verify the existence of all the other freedoms.' However, identifying only 17 articles with this positive view among the publications of six relevant British newspapers over a period of 10 years indicates the limitations of this approach. This number gets the right perspective considering that this research includes 833 newspaper articles about the Deep Web technologies, and 58 of them mention Tor.

Contemplating these 17 examples, the articles show some relevant effort to defend people's civil liberties. Furthermore, critical discourse analysis shows that the British press offer a liberation technology point of view based especially on the discussion of issues related to freedoms. Criticising state censorship and surveillance, for instance, is related to freedom of information, although there is a clear separation between the use of Tor to fight authoritarianism abroad, in China or the Middle East, and its use in the context of a democratic society such as the United Kingdom. British newspapers offer a much clearer opposition to the first issue, as happens in other matters (Collins et al., 2011). In addition, discussing privacy issues is related to protecting personal freedoms, human rights and dignity. Supporting online anonymity and defending activism are linked to various freedoms, such as expression, speech and information. Therefore,

[163] Read more about the values of the organisation Reporters Without Borders on https://rsf.org/en/our-values Access: August 2019.

the British press help protect people against state abuse and private interference by addressing how useful Tor can be in escaping online surveillance and reassuring civil rights (Loesing, 2009).

Moreover, these articles provide balance to the overall coverage of this topic, with a new perspective that shows a diverse range of arguments and an attempt to fill the educational role of the press. There are instances, however, in which these articles transfer the responsibility from the state to the people when discussing surveillance issues. Instead of addressing the problem of state control through the abuse of authorities, in both democratic and undemocratic regimes, these articles transfer to regular Internet users the burden of finding a solution. In this context, Tor is the miraculous response, since by using this network, users can achieve online privacy and anonymity, protect their communications and maintain regular activities. Although part of the news acknowledges censorship as an issue and provides examples of educative approaches, instructing people to protect themselves, this is more a reactive attitude to the situation than a proactive discussion of the limits of the power of the state and how personal data are being used nowadays. Furthermore, an article published by *The Guardian* even states that 'if you can avoid social networks altogether, that should also increase your privacy.'[164]

Reducing bias in coverage also contributes to a less stigmatised idea of what constitutes a Deep Web user, which can potentially increase awareness of current surveillance issues as well as promote privacy-granting technologies. Suggesting Web users in general download Tor to defend themselves is an audacious step in the direction of disseminating the existence of technologies developed to protect communications. But how easy is to adopt this kind of technology? At first glance, Tor appears to be just a simple piece of software to download, install and access, since the project's website explains step-by-step how to do it, but its usability depends on the user's experience (Van Hout & Bingham, 2013). Another problem is that Tor is time-consuming. According to Guitton (2013, p. 2813), 'the current technical know-how required to access the hidden services and the current speed of the Tor network make this option, at the moment, not worth considering for most users.' On the subject of global access to these tools, Diamond (2012, p. 15) even suggests that 'rich liberal democracies need to do much more to

[164] Related article: "Protecting yourself: delete, or block? How to avoid giving too much away," The Guardian, 2nd March 2012, Home Pages, page 19.

support the development of such technologies, and to facilitate (and subsidize) theirs cheap and sage dissemination to countries where the Internet is suppressed.'

Another point to highlight is that *The Guardian* coverage stands out in the context of positive articles about Tor. From 17 articles, 13 were published in this newspaper, which represents 76.4% of the total. There is a good explanation as to why *The Guardian* presents a more positive view of this technology than the other newspapers: their journalists had to use Tor to communicate with sources during the publication of the Snowden files. Furthermore, *The Guardian* was chosen as a newspaper that would help the topic gain global coverage, since WikiLeaks 'collaborated with numerous news organizations to release and report on its leaks, most prominently the *New York Times* and *The Guardian*' (Coddington, 2014, p. 683). This collaboration not only shows that this newspaper was willing to help investigate state abuse as well as report this to society, but it also improved its reputation as a newspaper that scrutinises sensitive issues (Cole, 2015). Therefore, considering also the historical socio-political approach of *The Guardian* (Wring & Deacon, 2010), it was expected that this newspaper would maintain a positive view and attitude towards privacy-enhancing technologies.

Finally, The Tor Project presents its own software in an extremely positive way, namely as a solution to fight censorship, avoid detection, achieve anonymity, obtain online freedom and enjoy many other civil liberties. These appear to be reasonable motivations to use Tor and defend its existence. Of course, its developers will indeed highlight the benefits it provides, in the same way that no one would expect Mark Zuckerberg to focus on Facebook's weaknesses, for instance. Adopting a positive discourse about Tor, though, the British press show that they can offer equitable coverage, but it is not necessarily the expected approach. As a matter of fact, Tor has consistently protected people everywhere (Bellare & Rogaway, 2005; Cammaerts, 2013; Dingledine et al., 2004; Grey, 2016; Loesing, 2009; Moore & Rid, 2016); however, as a privacy-granting technology that offers online anonymity, it is also used for criminal and antisocial purposes (Abbasi & Chen, 2007; Al-Rawi, 2019; Baker, 2015; Bleakley, 2019; Chen et al. 2008; Greenberg, 2016; Hossain, 2015; Mackey, 2018; Martin, 2014; Negri, 2016; Qin et al., 2005; Smirnova & Holt, 2017; Weimann, 2016a; 2016b). Therefore, acknowledging the multiple perspectives of this technology is the media's ethical obligation, because providing a diverse set

of angles strengthens and improves the discussion. Furthermore, the opposition between the positive and negative uses of this technology is such a strong part of Tor that the next chapter of this thesis is dedicated to studying this very notion.

7 The Tor Network, Technological Ambivalence and Polarisation

In an interview with the World Innovation Summit for Education[165] in 2014, the North American philosopher Noam Chomsky offered an insightful argument about technological ambivalence: '[A]s far as technology itself and education is concerned, technology is basically neutral. It's like a hammer. The hammer doesn't care whether you use it to build a house or whether on torture, using it to crush somebody's skull, the hammer can do either.' As the example of the hammer, the Tor Network can be used for noble and cruel purposes according to social, cultural, political and economic contexts. This technology enables online anonymity and privacy, which are used for competing reasons: defending democracy (Cammaerts, 2013) and buying drugs (Baker, 2015; Mackey, 2018; Martin, 2014; Negri, 2016; Smirnova & Holt, 2017); fighting authoritarian regimes (Jardine, 2018a) and distributing child abuse material (Bleakley, 2019); protecting vulnerable people (McLeod, 2011) and selling guns to terrorists and far-right movements (Abbasi & Chen, 2007; Al-Rawi, 2019; Chen et al., 2008; Greenberg, 2016; Hossain, 2015; Qin et al., 2005; Weimann, 2016a; 2016b) and so on.

Diverse uses and associations turn Tor into a complex topic addressed through the usual polarisation constructed by traditional or social media, and characterised for defending a point of view and undermining the opposite perspective (Doğu, 2017; Lee, 2016; Spohr, 2017). Drawing from critical discourse analysis in newspaper articles mentioning both the positive and the negative uses of Tor, as well from articles alluding only to negative uses, this chapter calls for taking a more balanced approach to this technology, even embracing its contradictions. Pointing to conceptualisations of ambivalence in regard to technologies, as well as more generally from a moral and epistemological point of view, this thesis finally argues that Tor is neither completely bad nor completely good but undeniably a necessary tool.

To provide some background to how Tor is represented overall, it is relevant to establish that the British press have offered limited coverage of this technology. Although Tor was developed

[165] Available on http://learning-reimagined.com/noam-chomsky-on-technology-learning/ Access: August 2019.

in 2002, the first publication on the topic occurred only in 2008. In total, in the six analysed newspapers – *Daily Mail*, *Daily Mirror*, *The Sun*, *The Daily Telegraph*, *The Guardian* and *The Times* –, 58 articles were published over 10 years. Data were collected between 2008, when the first article about Tor was published, and 2017. From this total, 17 mention only positive uses of Tor and were analysed in the previous chapters from the perspective of newspapers adopting a liberation technology discourse. This chapter looks at the other 27 cases in which its uses are mentioned: 15 articles referring to both positive and negative uses, and 12 articles alluding to only negative uses. As such, this analysis presents findings relating to an examination of newspaper articles, using a combination of content analysis and critical discourse analysis, which is feasible due the limited amount of cases. The remaining 14 articles from the total of 58 publications about Tor ignore the potential uses of this technology and are not considered further. This analysis is relevant to understanding not only how the ambivalence to Tor is addressed, but also how this is still used to suggest polarisation.

Thus, this chapter is organised in five main sections. The first section discusses the concept of technological ambivalence, and especially the context of the Web. The second focuses on how British newspapers present the ambivalence to Tor, examining this technology's portrayal through articles that mention positive and negative uses. The third section analyses the same articles to understand the tone of the arguments used to describe Tor and to discuss if presenting negative and positive uses results in unbiased coverage. The fourth section examines the 12 articles exemplifying an exclusively negative representation of Tor, connecting it to criminal and antisocial behaviours and uses. And the final discussion opposes positive and negative perspectives of Tor in the British press, to establish an overall discourse on the topic and to provide new insights into how this technology is represented.

7.1 On the Concept of Technological Ambivalence

'In the end, technology is merely a tool, open to both noble and nefarious purposes,' argues Diamond (2012, p. 5). A similar view is seen in Feenberg (1990), who uses the example of a factory to differentiate machinery potential from the purposes of those who control the same machinery, a Marxist perspective of technology also based in neutrality – the means of

production are neither good nor evil, although the people controlling them can impose equality or class struggle. Both perspectives centre on how technology is used – for private reasons or to promote general welfare – and not only what this technology enables people to do. Nevertheless, according to Feenberg (1990, p. 36), there are at least three reasons why technology is 'badly employed': harming people, negligence and not contributing to improving or protecting social values. As these arguments demonstrate, technological ambivalence is centred on the user and can vary according to social circumstances.

According to Moore (2006, p. 11), in the context of technological progress, ambivalence is related to people 'realizing that each time we take a step to make our world more efficient and productive, we also take a step toward a world in which we ourselves are a smaller and smaller part of a massive machine.' In addition, Locke (2005, p. 33) looks at the representation of science and technology to define 'the ambivalence about science as a source both of tremendous power and of equally tremendous threat.' On the same topic, Schraube (2009, p. 309) discusses how technological advances provide materialised power to things, therefore 'denying the ambivalence of technology would be the equivalent of denying human subjectivity. It blinds us to the role of technology in today's power, subjugation, and discrimination. It blinds us to a need to resist things and reflect on our own place in relation to them.'

With an opposing argument, however, Postman (1997, p. 229) claims that this perspective is naïve, in that 'of course, like the brain itself, every technology has an inherent bias, has both unique technical limitations and possibilities; that is to say, every technology has embedded in its physical form a predisposition toward being used in certain ways and not others. Only those who know nothing of the history of technology believe that a technology is entirely neutral or adaptable.' Postman (1997) also argues that since technological development is aligned with the expectations of dominant elites, new tools are constructed to ensure political and economic power. Nevertheless, according to Postman (2004), societies must have a sceptical attitude towards new information technologies and avoid early conclusions based on speculation about potential results while tools are being developed – what is seen as a solution in the first instance can raise even greater social problems later on.

Ambivalence has also been discussed as a social, moral and epistemic stance beyond the issue of technology. On the topic of social ambivalence, Bauman (1990, p. 151) debates modern societies' struggles with antagonism, which are anomalies in comparison to the regular order, suggesting that 'the opposition, born of the horror of ambiguity, becomes the main source of ambivalence.' Arribas-Ayllon & Bartlett (2014, p. 347) address sociological ambivalence by relating it to the potential of social and cultural actions, since 'ambivalence conceptualizes the positivity of knowledge and experience: it explores what forms of experience are possible and practicable within a given structure of social relations.' Considering the role of ambivalence in epistemology, Arribas-Ayllon & Bartlett (2014, p. 347) go on to contend that 'contradictions, paradoxes, disputes and controversies are intrinsic aspects of science-making.' Therefore, it is socially acceptable to portray something in a good or a bad way, but not both.

In the context of the Web, Tim Berners-Lee anticipated in 1996 the potential long-term implications of his invention, asking, 'What will happen to our cultures when geography becomes weakened as a diversifying force? Will the net lead to a monolithic (American) culture, or will it foster even more disparate interest groups than exist today?'[166] After 30 years, studies focusing on outcomes of the Web have proven that Berners-Lee's concerns were grounded, and ambivalence towards uses of this technology has emerged in broad public discussions as well as in the everyday experiences of many users. Although the Web is used for collaboration and the exchange of knowledge, and allows 'collateral benefits' on economic, cultural and social levels (Van Deursen & Helsper, 2018, p. 2344), it also enables distinct crimes (Bartlett, 2015), creates new kinds of harassment such as trolling (Coleman, 2014) and facilitates the distribution of fake news affecting democracies (Vargo et al., 2018), among other consequences. According to Bucher (2019, p. 3), the ambivalence of digital technologies and their potential role in societies must be approached with criticism and transparency whilst also understanding that new technologies cause social anxieties and worries as well as 'the legitimacy of believing in different (even contradictory) things at the same time, in an attempt to reorient our scholarly sensibilities toward the productive potentials of the ambivalent position.'

[166] Available on https://www.w3.org/People/Berners-Lee/1996/ppf.html Access: June 2019.

Furthermore, the Web is constantly studied in terms of its ambivalence. Kutscher & Kreß (2018, p. 3) research the potential impact of social media being used by minor refugees arriving in Europe to identify 'ambivalent challenges in a situation where their identity development experiences a precarious contextualization, especially in societies where right-wing political movements are on the rise.' There are many ambivalences on Facebook, one of them being that this platform works as 'an archive of life narratives and key moments' (Robards & Lincoln, 2016, p. 1), which adds a performative layer to relationships and raises issues with digital traces. Search engines also provide clear examples of ambivalence in their services (Andersen, 2018): on the one hand, they organise information in databases and facilitate access to these data, and on the other hand, they contribute to deep mediatisation, since social knowledge is constructed through searches, and search results are actually a business. In regard to people's ambivalence towards technology, as Contractor, Weiss & Elhain (2019) argue, it is very clear in smartphones. Although the devices can help with productivity enhancement, information-seeking, contact with family and friends and also for distraction, there is still a reasonable and grounded fear related to its use, once it can be connected to addictive behaviours such as problematic smartphone use (PSU), which has post-traumatic stress disorder (PTSD) symptoms.

This relevant ambivalence has also been explored regarding the Deep Web, especially in discussions related to the Tor Network. According to Jardine (2018a, p. 2828), 'it is certainly more than possible to get into trouble on the surface web, but it is also fairly likely that most people are using Tor to access legal and licit services with technological protections that help to ensure their privacy and anonymity rather than attempting to undertake outright illegal activity.' As Jardine (2018a) argues further, not only the Tor Network, but also the whole Web can be seen through a cloak of ambivalence, opposing negative and positive uses.

To what extent does this double dimension of Tor, and more generally the Deep Web, also emerge in press articles in the corpus examined herein? As shown in the previous chapters, an overwhelming majority of the articles tend to avoid ambivalence, in order to provide a negative or, more rarely, a positive representation of the Deep Web. However, very few articles present narratives and opinions that may be described as technological ambivalence. The next section of

this chapter addresses such cases, analysing newspaper articles presenting both positive and negative uses, and therefore both sides of this technology.

7.2 Ambivalence and the British Press's Representation of Tor

On the matter of how technological ambivalence is generally signified, it is worth noting that 'as much as technology is represented as a source of wonderment, so also – and often at the same time – is it represented as a source of worry' (Locke, 2005, p. 37). Furthermore, this opposition between wonderment and worry is identified in British press coverage of the Tor Network in a way that is not seen for the Deep Web in general, as discussed in Chapters 4 and 5. As the following analysis shows, articles recognising both views – positive and negative – suggest that Tor is neither completely good nor completely bad per se. Despite the tendency toward polarisation, evident in the quantitative analysis developed in Chapters 4 and 5, the media still provide more than one perspective on the uses of this technology, which makes sense in a context in which 'popular conceptions of idealized journalism are inherently predicated on the "Twin Towers" of unbiased reporting – balance and fairness' (Schaefer & Fordan, 2014, p. 275).

To show how the media deal with these multiple angles of Tor, this research identified 15 cases of an ambivalent approach to this technology in British newspapers. Table 15 presents these cases, organised in chronological order, specifying the arguments that are used to introduce positive and negative uses of Tor:

Table 15: Ambivalence of Tor in British newspapers

CASE DETAILS	POSITIVE USE	NEGATIVE USE
Case 1 The Daily Telegraph 27th October 2011	"helps dissidents in Iran and China to circumvent online censorship and surveillance"	"helps paedophiles avoid detection"
Case 2 The Guardian 21st April 2012	"huge degree of protection, whether to activists working on oppressive regimes"	"make regulating the internet an impossible task"

		"those using the internet to smuggle drugs or share child pornography"
Case 3 Daily Mail 27th January 2013	"used by FBI and championed by advocates of internet freedom" "safe channel to Egyptian dissidents during the Arab Spring and is used by bloggers in Syria"	"grants access to a world where the illegal is openly traded" "Tor users in the UK openly offer weapons, high-grade cocaine and brides for sham marriages. Cyber criminals also advertise their wares"
Case 4 The Guardian 23rd March 2013	"it is a staple of activists avoiding internet censorship or government crackdowns the world over, including in China, Iran and Syria"	"Silk Road runs as a 'hidden service' on a popular internet anonymising tool known as Tor"
Case 5 The Times 6th August 2013	"it is a vital resource to maintain the privacy of internet users, such as political activists in the Middle East who want to be able to speak freely on the web without fear of reprisals" "those who live under repressive regimes"	"has been used by arms traders, drug smugglers and child abuse rings to communicate without the risk of detection" "individuals and organisations that facilitate child abuse content"
Case 6 The Guardian 5th October 2013	"to keep it anonymous and avoid online censorship tools" "wide use in countries where there is routine surveillance or censorship of the internet"	"also used by people engaged in terrorism, the trade of child abuse images online drug dealing" "very naughty people use Tor"

	"used by dissidents in Iran, China, etc"	
Case 7 The Guardian 18th November 2013	"many of these will be carrying out perfectly legal activities"	"a favoured tool for those involved in distributing child abuse material, who have an interest in keeping their identities hidden"
Case 8 The Daily Telegraph 19th November 2013	"developed for noble reasons according to an open ideal" "many opposition voices under oppressive regimes would be silenced without Tor"	"used for nefarious activities" "taken over by people who want to use anonymity to mask less heroic activity" "used to buy anything from chocolate bars to crack cocaine"
Case 9 The Times 1st August 2014	"include journalists reporting from war zones, whistleblowers, democracy campaigners"	"criminal gangs"
Case 10 The Times 4th September 2014	"on the side of privacy"	"it's also the answer, unfortunately, for drug dealers and child pornographers"
Case 11 The Daily Telegraph 12th December 2014	"whistle-blowing sites and human rights information for activists around the world"	"vast amounts of child pornography, illegal drugs markets" "people will use it to keep sharing illegal pornography"
Case 12 The Times 11th August 2015	"originally created by American intelligence agencies to protect anonymity of their agents"	"anyone can access the dark net by downloading Tor"

Case 13 The Times 18th April 2016	"investigative journalism, freedom of speech, whistleblowing, private massaging and legitimate commerce as areas that can benefit from privacy without there necessarily being any wrongdoing involved" "people living under oppressive government regimes also use it to access media and communication tools that are banned on their country's conventional internet"	"criminals are usually keen to keep out of jail so they seek out technologies that offer privacy and anonymity"
Case 14 The Times 8th May 2017	"created to avoid the surveillance of tyrannies"	"it enables illegality, from pornography to financial fraud and drug dealing. Yet the lawlessness that allows these activities also allows predation upon those who indulge in them"
Case 15 The Times 8th May 2017	"providing security on the internet for all" "used for day-to-day internet access in countries with repressive governments and the Tor Project receives funding from the US State Department for this purpose"	"the murky online no man's land of the dark net, which is accessible only through a system called The Onion Router, or Tor"

The arguments organised in Table 15 help to unveil how opposing ideas and uses related to Tor are presented by the British press. Thus, this research identifies that a recurring approach of

the media is not only mentioning both aspects, but directly antagonising the positive and negative uses of Tor. Case 2, for instance, shows an article from *The Guardian* entitled "The internet is our most liberating tool, and the best for surveillance,"[167] which discusses Tor's ambivalences as a 'dilemma' (line 1). The use of this expression means that both alternatives – Tor being and not being available to the public – are undesirable: when Tor is available, criminals use it, and when it is not so, people that need online anonymity to escape censorship have no alternative.

```
1 This dilemma has not gone unnoticed by the people behind the tools. "Criminals
2 will always be opportunists and will see new prospects before everyone else
3 does," says the Tor project's executive director, Andrew Lewman.
```

This case also offers an argument based on technological ambivalence to put Tor's uses into perspective. This reason is attributed to a member of The Tor Project:

```
1 "The benefits of the open internet work much the same as motorways or
2 interstates: they outweigh the costs. In the US, police opposed the building of
3 interstate roads, saying they would help criminals circumvent the law. But the
4 police adapted, and the benefits of highways clearly outweigh the costs."
```

Furthermore, this argument suggests that the crime always finds a way of circumventing policing and surveillance, which is why they happen on the Surface Web as well as on the Deep Web. For Andrew Lewman, analysing the benefits and costs of the technology suggests that the existence of Tor is as valid as the development of highways. The same discussion about its ambivalence is addressed in Case 4, which presents an article from *The Guardian* entitled "Following the Silk Road: the drug dealers' eBay worth £1m a month"[168]:

```
1 The legitimate uses of Tor make disrupting the service morally difficult: it is
```

[167] Related article: "The internet is our most liberating tool, and the best for surveillance," The Guardian, 21st April 2012, Home Pages, page 24.
[168] Related article: "Following the Silk Road: the drug dealers' eBay worth £1m a month," The Guardian, 23rd March 2013, Home Pages, page 18.

```
2 a staple of activists avoiding internet censorship or government crackdowns the
3 world over, including in China, Iran and Syria. Indeed, a large proportion of
4 Tor's funding comes - albeit indirectly - from the US state department's
5 internet freedom budget.
```

This extract shows the relevance of Tor by citing the funding related to the 'US state department's internet freedom budget' (lines 4 and 5). The connection to this budget links Tor to an idea of internet freedom and frames this technology in a positive way, while the fact that it is openly funded by a liberal government indicates the benefits of its use. Moreover, the use of the expression 'morally difficult' (line 1) makes a strong case in the defence of Tor as an option for people who need protect themselves online – those who would like to disrupt Tor or make it illegal, in this sense, are considered immoral and as taking the wrong side. In this case, there is no dilemma, because the right side to be is the side of Tor's availability.

Presenting both uses of Tor provides examples of a balanced approach to the technology, such as in Case 7, an article published by *The Guardian* in November 2013 and entitled "Google targets online child abuse."[169] This article defines Tor by using neutral terms such as 'encrypted and anonymous networks' and 'anonymising service,' which are technically accurate. In addition, it connects the use of this technology to the rise in awareness about privacy issues, citing directly the 'US National Security Agency's activities' and its surveillance agenda as a justification. Finally, the publication also offers a neutral definition of the Dark Web, stating:

```
1 Sites are deliberately hosted in such a way as to be inaccessible by
2 conventional means through the open internet, and they cannot be found by
3 standard search engines.
```

This article, however, does not ignore that Tor has negative uses, alluding to the idea that it protects the identity of criminals distributing child abuse material. This case presents a very extreme example of the negative uses of Tor, related to paedophilia, a crime that meets with general disgust. Therefore, it does not soften the negative uses that can take place, and both

[169] Related article: "Google targets online child abuse," The Guardian, 18th November 2013, Home Pages, page 4.

opposing uses are addressed in seriousness. This approach is seen also in Case 11, an article from *The Daily Telegraph*[170] which summarises the ambivalence of Tor users: '[I]n short, people who either want or need to hide.' Another example of this duality is Case 10, an article from *The Times*:[171]

```
If you are afraid of Big Brother, be it the CIA or Tesco, the answer seems to
be to download the anonymising Tor browser. It is also the answer,
unfortunately, for drug dealers and child pornographers.
```

In a distinct approach, Case 6 is an example in which the negative uses of Tor are indeed mentioned, but its overall argument strongly defends the use of the tool. Entitled "NSA's attempt to crack web privacy tool used by dissidents is revealed"[172] and published by *The Guardian*, this article reports critically on attacks made by the NSA against privacy-enhancing technologies, as unveiled in the Snowden revelations. This article points to the irony of the United States government, on the one hand, sponsoring Tor, and on the other hand, trying to break the technology, raising concerns among privacy and human rights groups. In addition, It also unveils secret documents that mentioned Tor as 'the king of high-secure, low-latency internet anonymity' and includes the following statement in which the NSA not only confirms that is trying to break the Tor Network, but also that it will keep doing it:

```
In a statement, the NSA said: "In carrying out its mission, NSA collects only
those communications that it is authorised by law to collect. It should hardly
be surprising that our intelligence agencies seek ways to counteract targets'
use of technologies to hide their communications. Throughout history, nations
have used various methods to protect secrets, and today terrorists,
cybercriminals, human traffickers and others use technology to hide their
activities. Our intelligence community would not be doing its job if we did not
try to counter that."
```

[170] Related article: "Laws aren't the only solution to child porn," The Daily Telegraph, 12th December 2014, Editorial, page 27.
[171] Related article: "This trip to the zoo is lacking in animal magic," The Times, 4th September 2014, Features, page 10.
[172] Related article: "NSA's attempt to crack web privacy tool used by dissidents is revealed," The Guardian, 5th October 2013, Home Pages, page 2.

A general argument in favour of Tor is also seen in Case 13, an article published in *The Times* and entitled "Shining a light on web's darkest corners"[173]:

```
According to Mr Chappell, interest in the criminal side of the dark web has led
to the more positive connotations of having an anonymous online space being
overlooked. "There is an underlying assumption by many, including in some parts
of the media, that all content on the 'dark web' is criminal. This is not the
case." He cites investigative journalism, freedom of speech, whistleblowing,
private messaging and legitimate commerce as areas that can benefit from
privacy without there necessarily being any wrongdoing involved.
People living under oppressive government regimes also use it to access media
and communication tools that are banned on their country's conventional
internet. Facebook, for example, is still available, via Tor, the most popular
software tool for accessing the dark web. "What underpins all of these
endeavours, be they legitimate or criminal, is the desire for privacy and
anonymity," Mr Chappell says. "We monitor criminality across the web and we
find it in all parts of it including the surface. It is an internet-wide
problem, rather than exclusively a problem limited to just the technologies
that are labelled with the dark web. Criminals are usually keen to keep out of
jail so they seek out technologies that offer privacy and anonymity."
```

Following an explanation about how crypto markets work, and the challenges of policing the content available on Tor, the extract above offers an overall positive view of the technology through clarifications provided by a cybersecurity expert. In this example, it is clear that the Dark Web as well as Tor are not exclusively used to commit crimes, and the Surface Web is frequently used for criminal purposes, i.e. 'it is an internet-wide problem' (lines 14 and 15). This argument is not only well sustained through a list of examples of legitimate uses, but it is also captivating in the sense that it instigates critical thinking about the Web in itself. In general terms, it is clear that shutting down Tor would not be enough to make the Web a more positive environment, because criminals would adopt alternatives to fulfil their needs.

Some articles question Tor's availability to the public and argue that it should be restricted. This is what happens in Case 3, for instance, in the article "Drugs, guns, credit cards: everything

[173] Related article: "Shining a light on web's darkest corners," The Times, 18th April 2016, Business, page 45.

is for sale"[174] published by *Daily Mail* in January 2013, which addresses Tor as a 'controversial browser.' In the overall argument of the article, positive uses do not compensate for the negative ones, which is why Tor is called the 'dark domain,' connected to a harmful application and enabling activities that are 'highly illegal,' whereby hyperbole is used to take a position, since the law is absolute. This article also offers other expressions that reinforce negative aspects of anonymity, such as 'totally untraceable,' 'effectively invisible' and 'safe channel' – again using a discourse with language resources that illustrate potential uses of the technology.

Another example is Case 1, an article published in 2011 by *The Daily Telegraph* and entitled "The digital underworld,"[175] which presents a vilifying discourse about Tor. While explaining how it works and how layers of encryption are added to the access process, this article uses the expression 'that obscure its true source,' which connects the system not only to the idea of shadows and darkness, but also to something erroneous or fallacious. In addition, the article refers to the Surface Web as 'normal circumstances on the web,' also contributing to the overall picture that Tor is an anomaly. Finally, it also indicates with irony the fact that Tor is legal – once again questioning if this technology should actually be available to everyone – and reinforcing that it was invented by authorities as a privacy protection tool, so the other uses are seen as negative and unexpected outcomes.

This can also be seen in Case 8, an article from *The Daily Telegraph* entitled "Abuse: the net is closing"[176] and published in November 2013. In this example, there is a set of associations between Tor and negative uses, concepts and ideas. The extract begins by opposing 'noble reasons' behind the Web's development and the 'nefarious activity as well as good' that Tor allows to happen. The second paragraph provides an explanation about how this technology works, with a brief precis of the encryption process, in which it mentions the onion analogy when talking about 'innocent addresses' that receive 'layer after layer of obfuscation.' Although the article states that 'many opposition voices under oppressive regimes would be silenced without

[174] Related article: "Drugs, guns, credit cards: everything is for sale," Daily Mail, 27th January 2013, no page number.
[175] Related article: "The digital underworld," Daily Telegraph, 27th October 2011, Features, page 35.
[176] Related article: "Abuse: the net is closing," The Daily Telegraph, 19th November 2013, Opinion, page 21.

Tor,' it reinforces that this tool is also used 'to mask less heroic activity.' Therefore, the overall discourse shows an expressed disapproval of Tor.

Case 5 shows an example from *The Times* whereby an article published in August 2013 and entitled "FBI acts to close thousands of hidden child abuse sites"[177] presents Tor as a technology that 'masks' and 'protects online identities,' terms that use both positive (protection) and negative (mask) wording. However, when the article presents the argument that Tor can be used to protect users' privacy, citing as an example 'political activists in the Middle East,' this sentence is connected to 'its supporters say,' which imputes some distance between the beliefs of the article's author and a possible justification for Tor's availability. This is seen also in Case 12, from *The Times*, in which the positive outcome of protecting soldiers in war zones is only mentioned to explain why Tor was developed, whilst the rest of the article, entitled "Hearts of Darkness,"[178] takes a condemning approach to online anonymity.

In Case 14, an article entitled "Unsafety Net"[179] by *The Times*, as the title suggests, the overall argument is that paedophiles use Tor to protect themselves, but this technology was created against 'the surveillance of tyrannies.' This is the only mention of Tor in a positive light. The same is seen in Case 15, published on the same day and by *The Times*, which focuses on child abuse. Entitled "Hello, paedophiles, you've been hacked,"[180] this article presents a strong case against the Dark Web but includes a brief defence of Tor's existence:

```
Duncan Campbell, a specialist in computer forensics, said that despite the
protections offered by Tor, users often made mistakes that would tip police off
as to their identities. The authorities could then use new variations on old-
fashioned investigative techniques to gather evidence. Mr Campbell is adamant
that there would be nothing gained by outlawing encryption or banning the Tor
technology. "Providing security on the internet for all is like providing motor
cars for all. Some people will use them for evil," he said. "There is no magic
technical solution that will make the problem go away."
```

[177] Related article: "FBI acts to close thousands of hidden child abuse sites," The Times, 6th August 2013, News, page 6.
[178] Related article: "Hearts of Darkness," The Times, 11th August 2015, Editorial, page 25.
[179] Related article: "Unsafety Net," The Times, 8th May 2017, Editorial, page 21.
[180] Related article: "Hello paedophiles, you've been hacked," The Times, 8th May 2017, News, page 11.

More than portraying Tor in a negative way, Case 9 adds a layer of fear and apprehension to the technology's use while reporting on Silk Road. The article entitled "Dark net drugs market doubles in size in a year"[181] and published in *The Times* includes the following extract:

```
1 Adam Benson, deputy executive director of Digital Citizens Alliance, said that
2 the internet could be "a wonderful tool for consumers and businesses" but "we
3 do worry [that] good people and companies get caught up in the web spun by
4 criminals and rogue operators. That will slowly erode the trust and confidence
5 we have in the internet." Internet experts caution against using Tor and other
6 dark net browsers because they give others direct access to the user's machine.
```

This excerpt offers concerns related to Tor using as a source a member of the Digital Citizens Alliance, an initiative designed to make people aware of the threats of the Internet. Including this source with no counterpart per se indicates that the overall argument of the article is connected to raising fears. As the extract shows, there is an idealised view of the Internet as a "'wonderful tool' (line 2) in which people have 'trust and confidence' (line 4). In this sense, opposition is presented between 'good people' (line 3) using the Internet and 'criminal and rogue operators' (line 4) using the Dark Web. Finally, the article ends with broad advice that is a 'caution against using Tor' from 'Internet experts' (line 5), thus arguing that Tor and other technologies are not safe, which discourages their use.

Overall, the positive perspective on Tor's uses acknowledges the current state of surveillance, especially in countries with authoritarian regimes, stressing that censorship requires the use of privacy-granting technologies enabling online anonymity, in order to assure freedom of speech and protect human rights, democracy and more generally internet freedom. Furthermore, this aspect of the discourse presents Tor as a liberation technology – as seen in Chapter 6. On the negative side, however, Tor is consistently represented through hyper-panic – a concept previously addressed in this thesis and related to a combination of media and moral panic, in which the media coverage of a medium multiplies existing fears. In this case, Tor is consistently

[181] Related article: "Dark net drugs market doubles in size in a year," The Times, 1st August 2014, News, page 24.

linked to cases of paedophilia, crypto markets, the illegal trade in drugs and arms, terrorism and other crimes.

As this section argues, newspaper articles use discourse to prove a point in the defence of or against Tor. One of these resources is comparison. When Tor is compared to other technologies and inventions that can also be used for criminal reasons, it shows that taking a stance against the tool in itself can be unreasonable. Another usual resource is to call for moral and ethical behaviours, explaining how Tor can protect lives, which in itself is a very emotional and appealing justification for the technology's existence and availability. Finally, a strategy used to counterbalance multiple uses in a positive way is to mention that lawbreaking occurs everywhere on the Web, not only on the Deep Web, and these misdemeanours are not enabled by Tor alone; therefore, imposing special control over this part of the Internet is not the solution to wiping out crime. In the next section, however, this research examines how newspapers use discourse to make a point, even when acknowledging both positive and negative uses.

7.3 A Matter of Tone

Although in some of these newspaper articles arguments can be considered opposing and counterbalancing each other, the fact that both sides of the argument are addressed does not mean that these papers present unbiased journalism, since polarisation is still perceived. Discussing media bias, Merkley (2008, p. 15) argues that 'there are many factors operating in newsroom environments that make it debatable whether this bias will manifest itself in practice. Perhaps the most important among them is that editors are tasked with providing content that sells.' Related to this idea of producing appealing content, Soroka et al. (2018, p. 1080) note that 'one of the most frequently identified tendencies in traditional media […] is the emphasis on negative information' as a way of attracting an audience. In this sense, a common approach taken by the media is seeing the glass as half-empty, and the Tor Network is one of the topics to which this pessimism is addressed.

To illustrate this point, this analysis considers not only arguments that are opposed in the article, but also the general tone that is presented. In the context of critical discourse analysis, tone is explained by Phelan (2014, p. 50) as 'the attitude the speaker takes toward the subject

matter of the utterance,' considering therefore 'narrative as rhetoric, that is, a multi-layered, purposeful communication from an author to an audience.' Presenting multiple sides of an argument is a way of showing journalistic independence, but it does not assure balanced coverage all the time, as the selection of views 'may contain an implied bias' (Venger, 2019, p. 3). Additionally, according to Venger (2019, p. 3), 'journalists have the power and means to construct alternative views by choosing to include the commentary of some sources and not others.' Moreover, offering multiple angles can cover the general hyper-panic tone of an article. Table 16 lists arguments included in the articles, to provide an overall tone for each example.

Table 16: Tone of ambivalent articles about Tor in British newspapers

CASE DETAILS	HEADLINE	TONE AND ARGUMENTS
Case 1 The Daily Telegraph 27th October 2011	"The digital underworld" (News article)	Overall negative "this is the lawless world of darknets" "this digital underworld has come to the attention of law-abiding web users thanks to an illegal, if arguably not immoral, act" "Tor users' internet traffic is bounced around a global network of computers that obscure its true source" "the irony of this is that Tor was invented by the US government and the software is legal, at least in the West" "so called hidden sites are not new and the system they use poses some challenges to law enforcement"
Case 2 The Guardian 21st April 2012	"The internet is our most liberating tool and the best for surveillance" (News article)	Overall positive "others aren't content merely to lobby politicians for a free internet. Instead, they have built tools designed to make regulating the internet an impossible task"

		"provides a huge degree of protection" "to give users control over how they use the internet and who is able to monitor their activity" "information should, generally speaking, be free"
Case 3 Daily Mail 27th January 2013	"Drugs, guns, credit cards: everything is for sale" (News article)	Overall negative "the dark web is a haven for criminal gangs around the world" "grants access to a world where the illegal is openly traded" "a dark domain that is used to host highly illegal marketplaces" "Tor users in the UK openly offer weapons, high-grade cocaine and brides for sham marriages. Cyber criminals also advertise their wares"
Case 4 The Guardian 23rd March 2013	"Following the Silk Road: the drug dealers' eBay worth £1m a month" (News article)	Overall negative "despite law enforcement authorities across the world being fully aware of its operation they have been powerless to stop it" "technological innovations that make it all but impregnable" "can you imagine if we had restrictions of speech, or the surveillance state, 400 years ago? We wouldn't have had the Reformation, or the Enlightenment, or the scientific revolution. Those would have been stopped - and we're having other kinds of revolutions now"
Case 5 The Times 6th August 2013	"FBI acts to close thousands of hidden child abuse sites" (News article)	Overall negative "users download special software that masks their identities" "going after the individuals and organisations that facilitate child abuse content is all to the good"

Case 6 The Guardian 5th October 2013	"NSA's attempt to crack web privacy tool used by dissidents is revealed" (News article)	Overall positive "a popular tool designed to protect online anonymity" "an open-source public project that bounces users' internet traffic through several computers, called 'relays' or 'nodes,' to keep it anonymous and avoid online censorship tools" "which law enforcement agencies say is also used by people engaged in terrorism, the trade of child abuse images, and online drug dealing" "wide use in countries where there is routine surveillance or censorship of the internet"
Case 7 The Guardian 18th November 2013	"Google targets online child abuse" (News article)	Neutral "the government estimates that 20,000 people are using encrypted networks, such as the Tor anonymising service, to communicate. Many of these will be carrying out perfectly legal activities" "awareness of the threat to privacy and knowledge of the 'dark web' have increased since news of the US National Security Agency's activities surfaced" "dark web is also a favoured tool for those involved in distributing child abuse material, who have an interest in keeping their identities hidden" "the technology used means that they do so with a high degree of anonymity"
Case 8 The Daily Telegraph 19th November 2013	"Abuse: the net is closing" (Opinion)	Overall negative "an example of a technology developed for noble reasons according to an open ideal, that has been used for nefarious activity as well as good"

		"software that masks the identity of internet users" "swaps those innocent addresses with those of people who want to hide their identities, encrypting and swapping them again and again, wrapping the information in layer after layer of obfuscation" "for individuals to be able to use it untraceably it must be open, which means it can be taken over by people who want to use anonymity to mask less heroic activity"
Case 9 The Times 1st August 2014	"Dark net drugs market doubles in size in a year" (News article)	Overall negative "masks their identity by running their connection through other computers on the network" "provide anonymised web connections" "Internet experts caution against using Tor and other dark net browsers because they give others direct access to the user's machine"
Case 10 The Times 4th September 2014	"This trip to the zoo is lacking in animal magic" (Opinion)	Overall negative "the answer seems to be to download the anonymising Tor browser" "it is also the answer, unfortunately, for drug dealers and child pornographers" "its (*the Web*) delinquency looks like rather more than a phase it is going through"
Case 11 The Daily Telegraph 12th December 2014	"Laws aren't the only solution to child porn" (Opinion)	Neutral "these have operated with such impunity for so long because they are hosted on servers using non-standard protocols that encrypt traffic to and from the site" "obscures that user's IP address"

		"but unless you bring down the entire Tor network - with all the good things it provides - people will use it to keep sharing illegal pornography"
Case 12 The Times 11th August 2015	"Hearts of Darkness" (Opinion)	Overall negative "a shadow web originally created by American intelligence agencies to protect the anonymity of their agents" "the technological challenge is too great" "intelligence agencies are engaged in an endless game of online whack-a-mole"
Case 13 The Times 18th April 2016	"Shining a light on web's darkest corners" (News article)	Overall negative "interest in the criminal side of the dark web has led to the more positive connotations of having an anonymous online space being overlooked" "criminals are usually keen to keep out of jail so they seek out technologies that offer privacy and anonymity" "the paradox about the dark web is that something designed to enable complete anonymity can be used so effectively to undermine privacy" "his study revealed the relative scale of nefarious activity on the dark web compared with more legitimate uses"
Case 14 The Times 8th May 2017	"Unsafety Net" (Opinion)	Overall negative "best understood as software designed to conceal their identities" "parts of the dark net are inherently lawless, with Tor having been created to avoid the surveillance of tyrannies" "it enables illegality, from pornography to financial fraud and drug dealing"

Case 15 The Times 8th May 2017	"Hello paedophiles, you've been hacked" (News article)	Overall negative "murky online no man's land of the dark net, which is accessible only through a system called The Onion Router" "Tor anonymises users' activity, making it impossible for authorities to track their IP addresses, the internet's equivalent of phone numbers" "before the dark net, logs showing the IP addresses of users of child abuse websites could lead police to suspects. That approach is closed off by Tor"

As Table 16 shows, out of a total of 15 articles mentioning the positive and negative uses of Tor, only two of them can be considered neutral, and in this sense, these articles allude to distinct uses as a dilemma, without prioritising one or other side. In Case 7, a neutral approach, an article published by *The Guardian* and entitled "Google targets online child abuse" presents both uses as 'perfectly legal activities' and 'distributing child abuse material.' This example explains that Tor provides 'a high degree of anonymity,' which is actually not portrayed as something bad or good. The same opposition is seen in Case 11, entitled "Laws aren't the only solution to child porn" and published by *The Daily Telegraph*. This example acknowledges that Tor is used for 'sharing illegal pornography' as well as 'all the good thing it provides,' which produces an unanswered dilemma.

Regarding positive approaches to multiple potential uses, just two cases highlight how Tor can be constructive, and they mainly discuss freedom of speech. In Case 2, for instance, an article by *The Guardian* opposes the liberation the Internet offers from surveillance issues caused by online technologies, and Tor is associated with terms such as 'free internet,' 'protection' and 'control.' The other example is Case 6, also published by *The Guardian*, which defends Tor for protecting people's identities but condemns the attempts of governments to break this tool. In this second case, although negative uses of Tor are mentioned, the overall tone of the article is

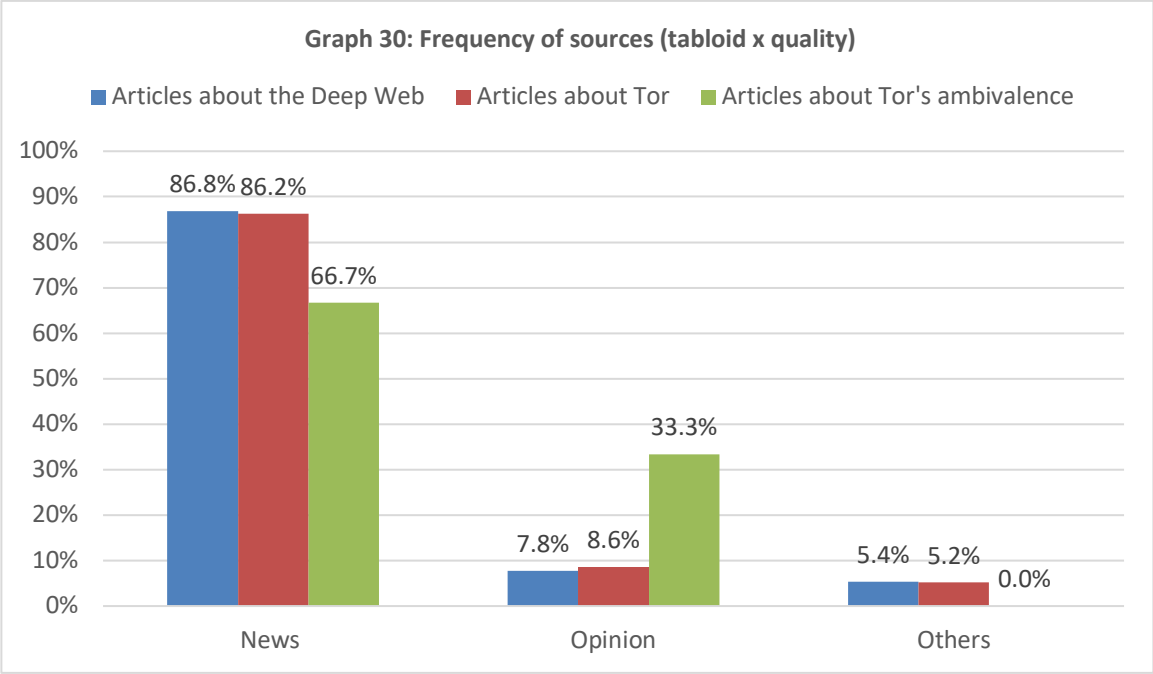
clear on the provided definition: '[A] popular tool designed to protect online anonymity. The use of the verb "protect" here, instead of "enable" or "allow," shows that Tor is seen as a defence tool and is thus viewed in a positive light.

The other cases, namely 11 articles from a total of 15, strengthen the connection between Tor and negative behaviours and uses. The idea that its objective is to circumvent the rules to protect criminals is seen, for instance, in Case 1, published by *The Daily Telegraph*, through the use of terms such as 'lawless,' 'illegal' and 'immoral.' It is also seen in Case 3, from *Daily Mail*, which compares Tor to a 'heaven for criminal gangs' while presenting a very negative frame of this technology. Published by *The Guardian*, Case 4 looks at undesirable outcomes of Tor from an official perspective, mentioning 'powerless.' In addition, Case 8 is related to an article published by *The Daily Telegraph* on child abuse material, which mentions a turn between Tor's initial purpose and its actual use, from 'noble reasons' to 'nefarious activities.'

Looking at the 11 articles that with a negative tone in relation to Tor, seven examples were published between 2013 and 2017 by the same newspaper, *The Times*, which 'leans to the right' (Lewis & Hunt, 2011, p. 165). Among these cases, negative approaches are taken in distinct ways. Case 5, for instance, defends intelligence agencies trying to seize Tor, arguing that it 'is all to the good.' It is worth mentioning here that the proximity between these agencies and the British press is common however problematised, because it can affect journalistic criticism and autonomy and thus the credibility of the press (Lashmar, 2013). The same argument is used in Case 12, which discusses Tor as a 'technological challenge' for the authorities, therefore questioning its public availability. Case 15 presents the same point, mentioning that is 'impossible for authorities to track.' In a more extreme example, Case 9 spreads overall fear of the technology by directly advising people not to use Tor. A similar vilifying approach is taken in Case 14, which calls it 'inherently lawless.' Finally, examples of how Tor is consistently associated with criminal uses are seen in Case 10, which connects Tor to 'delinquency,' and Case 13, which twists the technological aim and argues that Tor actually imposes challenges in relation to privacy, since cybercriminals can use it to break into people's devices.

Another element to consider is related to the type of article, if news or opinion, presenting Tor as ambivalent. As Graph 30 shows, comparing the total publications analysed in this thesis

(833 articles about Deep Web technologies), publications specifically about Tor (58 articles mentioning this technology) and those addressing its positive and negative uses (15 articles analysed in this section and the previous one), there is an definite variation in the last case. Although articles about Deep Web technologies and about Tor have a higher percentage of news (86.8% and 86.2%, respectively), this number drops to 66.7% in the case of articles opposing positive and negative uses, with a considerable increase in the number of opinion articles from 7.8% (articles in general) to 33.3%.



As noted by Hoffman & Slater (2007, p. 58), 'the exchange of opinions is an important component of participatory democracies, and newspaper forum pages have been hailed as a conduit for such discussion.' Additionally, Schmidt (2015) contends that opinion articles are more likely to be strongly biased, especially when compared to news articles in general. This is illustrated by Table 17, which shows the tone of articles portraying Tor's ambivalences. Considering the overall negative representation of Deep Web technologies, as analysed in previous chapters, it makes sense that opinions expressed in the media are also predominantly

negative. Furthermore, the only case in which there is a neutral approach is related to arguing about how Tor needs to be policed but not eradicated (Case 11).

Table 17: Tone of articles about Tor in British newspapers by type of article

	OVERALL POSITIVE	OVERALL NEGATIVE	NEUTRAL
OPINION	-	4	1
NEWS ARTICLE	2	7	1

As this section shows, presenting multiple uses of a technology does not mean that the media approach to it is neutral, because acknowledging other uses can be seen as a strategy to defend a specific frame or argument, or even a way of showing independence and non-bias. Furthermore, in the majority of the cases, the protection that Tor offers is seen as a threat to the work of authorities against cybercrime, suggesting polarisation of the discussion. Moreover, the positive practices of Tor are consistently mentioned as initial purposes but not actual uses: according to this portrayal, although Tor was developed to be a liberation tool and help with freedom of speech, the reality is that it helps criminals. There are rare cases in which this is portrayed as a dilemma, but, overall, fears and threats impose a stronger frame than the idea that Tor has legitimate uses. In the next section, this research looks at newspaper articles mentioning only the negative uses of Tor, to uncover what fears are directly connected to this technology.

7.4 When the Glass is Half-Empty

Understanding the ambivalence of Tor and media bias towards this technology requires unveiling negative perspectives and arguments presented by newspapers when they seem unable to acknowledge anything positive about it. As seen before in this thesis, the Deep Web is generally negatively represented by British newspapers through constant associations with criminal and antisocial behaviours (see Chapter 4), multiplying existing fears and introducing new ones, in a phenomenon that this research calls “hyper-panic” (see Chapter 5). This section

highlights articles about Tor that follow the same tendency. Although Chapter 6 suggests an overall attempt to present the positive uses of Tor, and the previous sections of the current chapter show how ambivalent views are balanced in daily coverage, this section examines cases in which using Tor is connected only to undesirable purposes, ignoring any positive outcomes. Each case in which newspapers articles mentioned only negative uses, totalling 12 articles, is listed in the following table, in chronological order:

Table 18: Negative uses of Tor in British newspapers

CASE DETAILS	NEGATIVE USE
Case 1 The Daily Telegraph 5th October 2013	"an alleged international criminal mastermind" "this involved setting up Silk Road in early 2011 using encrypted software, known as onion routing, invented by the US Navy"
Case 2 The Guardian 1st November 2013	"revelations about Tor and the dark web would help arms dealers and paedophiles"
Case 3 The Guardian 14th April 2014	"Silk Road was the largest online black market site in the world. The site was accessed via the anonymous web browser Tor"
Case 4 The Times 14th January 2015	"the site would be hosted on The Onion Router (Tor), an anonymous dark web network that already contains marketplaces selling guns, drugs and stole information"
Case 5 The Times 14th August 2015	"Tor, the dark web browser" "it provides online anonymity for dealers and buyers"
Case 6 The Times 31st October 2015	"to bulk buy stolen data at lower prices, however, fraudsters head to the dark web. This can be accessed via the Tor browser, rather than conventional browsers" "allowing would-be identity thieves to connect to hidden services"
Case 7 The Guardian	"technology becoming the 'primary facilitator' for lawbreaking, with entrepreneurial criminal start-up's

10th March 2017	mushrooming across the 'darknet.' This distributed anonymous network, accessible via software such as The Onion Router (TOR), I2P and Freenet is now the main supplier of raw materials for forged documents"
Case 8 The Times 5th May 2017	"the use of Tor anonymity software makes it hard for police to infiltrate an abuse forum"
Case 9 The Times 8th May 2017	"by using anonymising software called Tor they (*paedophile rings*) masked their online identities"
Case 10 The Times 7th August 2017	"The dark web is only accessible using a covert browser such as Tor, allowing users to be untraceable. The UK National Crime Agency (NCA) has said that the use of the dark web as a 'marketplace for firearms, drugs and indecent images of children' is rising"
Case 11 The Times 2nd September 2017	"criminals who engage in cyberblackmail often use Tor, a web browser that routes traffic through encryption software so users cannot be traced"
Case 12 The Times 21st September 2017	"a further problem is that most popular social media and file-sharing companies allow account managers whose identities are unknown to simultaneously use various technologies, such as virtual private networks and specialised browsers such as Tor, to mask their physical locations when active on their sites"

As Table 18 shows, mentions of negative uses of Tor reproduce what was observed during the analysis of activities connected to the Deep Web, namely episodic coverage and hyper-panic related to fears such as crypto markets (especially Silk Road), child abuse, terrorism and cybercrime, among other negative uses addressed by British newspapers. Discussing why audiences are so fascinated by crime, Cavender (2004, p. 338) argues that 'crime stories deal with mythic issues of good and evil, personalized in the character of heroes and villains; they create tension and then resolve it, which is pleasurable.' And according to Cavender (2004, p. 339), the way the media have represented crime since the 1970s has reinforced the relevance of the topic

and helped shape a common narrative adopted by societies: '[C]rime, in the real world, but also as depicted in the media, becomes a part of the agenda of public discourse.'

The fact that Silk Road was developed to work through the Tor Network, an so by default crypto market users need this technology to access the website, is a point of special interest among the British press. Case 1 is an example of how Silk Road is generally seen, with an article published by *The Daily Telegraph* and entitled "Hit men, drugs and the fall of the Silk Road 'mastermind'"[182] providing the following explanation:

```
The website was a digital black market bazaar for buying and selling every kind
of illegal drug, as well as counterfeit bills, fake passports and drivers'
licences, and stolen credit card information. Computer hackers advertised
services such as cracking into cash machines, as did hit men operating in more
than 10 countries.
```

As this extract shows, Silk Road is portrayed as the source of any possible crime on the Web: drugs, fake documents, stolen data, crime tutorials, assassinations. Although Silk Road was developed in the United States, its business was not restricted to this country, so Case 3 addresses the issue of drug consumption in the United Kingdom through the results of the 2014 Global Drug Survey in the article "It's official: the UK is a nation of hedonists."[183] This study revealed a shift from street dealers to online trade. Published by *The Guardian*, this article presents Silk Road as a leading figure in this change, including numbers related to awareness and access:

```
Almost a quarter of UK respondents to the survey - which is partnered by Mixmag
and the Guardian in the UK and is likely to be answered by people who take
drugs regularly - said they had bought drugs over the internet. Just under 60%
knew about Silk Road, and of these, 44% had accessed the site.
```

[182] Related article: "Hit men, drugs and the fall of the Silk Road 'mastermind,' The Daily Telegraph, 5th October 2013, News, page 21.
[183] Related article: "It's official: the UK is a nation of hedonists," The Guardian, 14th April 2014, Home Pages, page 3.

Silk Road is mentioned again in Case 5, in which the article "Dark web rakes in £115m a year from sales of drugs and guns"[184] published by *The Times* also mentions changes in the drug trade. Furthermore, the extract below shows that this change is not only connected to the crypto market, but Tor is seen as a weapon (line 3) against the police:

```
1 Analysis Tech-savvy drug dealers are moving from the street to the dark web to
2 seal themselves in a cloak of almost complete anonymity (James Dean writes).
3 Once they set up shop, they have two weapons to throw police off their trail:
4 Tor, the dark web browser, and bitcoin, the digital currency. Tor can be
5 downloaded free in minutes. It provides online anonymity for dealers and buyers
6 alike by masking internet connections through a web of other Tor users.
```

Also in relation to crypto markets, Case 6 discusses how stolen data are traded on the Dark Web, in an article published by *The Times* and entitled "Stole credit card details available for £1 each online."[185] On the same topic, Case 7 presents an article published by *The Guardian* on "Number of criminal gangs operating in Europe surges to 5,000m says Europol"[186] and quotes an official report to explain how technology helps crime. This article also presents a general message that crypto markets are seen as a threat by the authorities. Furthermore, it presents official numbers that estimate the criminal uses of the Deep Web as a very high percentage (see below). According to Owenson, Cortes & Lewman (2018), however, only 2% of the total network traffic is related to the Hidden Services – the ones in which, for instance, crypto markets are developed.

```
1 Every day, around 1.7 million people use the darknet, in which 57% of all
2 marketplaces and forums are devoted solely to criminal activity, according to
3 figures cited in the Europol threat assessment.
```

[184] Related article: "Dark web rakes in £115m a year from sales of drugs and guns," The Times, 14th August 2015, News, page 9.
[185] Related article: "Stole credit card details available for £1 each online," The Guardian, 31st October 2015, Technology.
[186] Related article: "Number of criminal gangs operating in Europe surges to 5,000m says Europol," The Guardian, 10th March 2017, UK News.

Another website accessible through Tor and mentioned by the media is The Slur (see Case 4). In this case, an article published by *The Times* and entitled "Military secrets for sale on dark web"[187] explains the development of a new website promising to combine WikiLeaks and Silk Road: a crypto market for the trade in classified information. The motivation of the website is explained in the following extract:

```
1 It claims that the financial incentives to sell secrets anonymously would be
2 more effective at uncovering private information than "the ideology that drove
3 patriots like Edward Snowden." Mr Snowden, a former contractor for the CIA,
4 faces espionage charges after leaking details of internet and phone
5 surveillance by American intelligence and has been granted asylum by Russia.
6 The site would be hosted on The Onion Router (Tor), an anonymous dark web
7 network that already contains marketplaces selling guns, drugs and stolen
8 information.
```

This article uses sentences from a statement made by the hacker group u99 to explain how this new website would work and, at the same time, make a point on its inconsistency. The sentences listed below show a questionable purpose in enabling people to trade information and make money from this practice, instead of using tools available on Tor to report misconduct, motivated by a principled pursuit of accountability.

```
1 "you are going to hate it"
2 "will bleed organisations' secrets and funds"
3 "a profound and lasting effect on our society"
4 "accessible by numerous disgruntled or psychopathic personnel"
5 "unflattering celebrity photos and videos"
6 "1,000 psychopaths willing to anonymously sell out their peers for material gain"
7 "incalculable resource for public knowledge and unfiltered access to the truth"
8 "to compensate whistleblowers for the extreme risks they take"
```

The use of the term 'psychopath' (lines 4 and 6), for instance, is connected to antisocial behaviour, lack of empathy and selfishness. Associating the website with this kind of approach

[187] Related article: "Military secrets for sale on dark web," The Times, 14th January 2015, News, page 15.

demonstrates that the purpose is actually negative. The choice of the verb "to bleed" (line 2) shows the violence in the discourse, since bleeding is a reaction to an injury. The pride in developing a website that will be hated (line 1) and at the same time change society (line 3) also shows the intent to cause an impact, for good or for bad. Although the group attempts to show some idealistic beliefs (line 7), the statement also exposes that crimes will be welcome (line 5) and, at the end of the day, the purpose is to make people pay for information (line 8). Using the words of this group, which has an aggressive approach and discourse, helps build an imaginary in which Tor is seen as a technology that facilitates violence and crime.

Crimes involving children or young people have a particular interest for the British press, and 'typically violent crimes are overrepresented in the media' (Collins et al., 2011, p. 8). This kind of crime is also connected to an emotional response, and so connecting Tor to these activities adds a negative layer to the technology. This happens in Case 11, for instance, in which the article "Officers cracked aliases of teen's online blackmailer"[188] published by *The Times* reports on how criminals use Tor to cover their tracks. Entitled "Hundreds of suspected paedophiles held after dark net forum is hacked,"[189] Case 8 presents an example from the same newspaper in which a website accessed through Tor is considered a refuge for people seeking content on child abuse:

```
1 The Playpen website, which operated through anonymous internet browsers,
2 offered 150,000 members a "safehaven" to view and trade child abuse imagery
3 without detection. Using software called Tor, its members were able to mask
4 their identities to access and distribute tens of thousands of illegal images.
```

According to this article, Tor raises concerns among authorities, which cannot break the technology, so investigations are conducted by infiltrating paedophile rings. This imposes a pertinent ethical discussion on the limits of what police and intelligence agencies can do to catch criminals:

[188] Related article: "Officers cracked aliases of teen's online blackmailer," The Times, 2nd September 2017, News, page 5.
[189] Related article: "Hundreds of suspected paedophiles held after dark net forum is hacked," The Times, 5th May 2017, News, page 14.

```
In Playpen's case, the FBI was criticised for running the site for almost two
weeks after gaining access. Although the operation collected data on thousands
of users, during the period about 200 videos, 9,000 images and 13,000 links to
child abuse were posted on the site. Defence lawyers and privacy campaigners
argued that the "outrageous conduct" involved the FBI engaging in illegal
activity itself. "They need to catch bad guys, yes, but I don't think the FBI
should be in the child porn distribution business," Christopher Soghoian, a
privacy researcher, said.
```

Child abuse is a topic to which Tor is consistently connected. For instance, Case 9's article "Child abuse network had 10,000 UK members"[190] published by *The Times* cites Tor as a tool for paedophiles. Taking a warning approach to how this technology works from the National Crime Agency (NCA) perspective, this article accuses Tor of enabling a 'proliferation of paedophiles sites.' A similar discourse that highlights the rise in the number of websites on the Deep Web is seen in Case 10, from the same newspaper and motivated by the same source, entitled "A sinister crime ring or fantasy?"[191] On the topic of whistle-blowing, Case 2 discusses the implications of Snowden's revelations with the article "The NSA files" [192] published by *The Guardian*. This example exposes the United States government's assumption that raising awareness of Tor would only be celebrated by criminals, ignoring that other people could use Tor with for legitimate purposes. The use of official sources adds a layer of concern to the coverage and increases the fear related to a topic because it is portrayed as a threat. Furthermore, Venger (2019, p. 2) argues that 'media accounts of major events rely on these sources for summary and interpretation' as well as 'how sources are used in the framing and validation of the story's content and message are a crucial component of the socio-political nature of news reporting.'

Finally, terrorism is also a source of moral panic usually associated with the Deep Web, and Tor is also seen as facilitating this kind of criminality. Case 12 is related to the article "Britain must lean on Trump to police terrorist websites"[193] published by *The Times*:

[190] Related article: "Child abuse network had 10,000 UK members," The Times, 8th May 2017, News, page 1.
[191] Related article: "A sinister crime ring or fantasy?," The Times, 7th August 2017, News, page 5.
[192] Related article: "The NSA files," The Guardian, 1st November 2013, Home Pages, page 8.
[193] Related article: "Britain must lean on Trump to police terrorist websites," The Times, 21st September 2017, Editorial, page 32.

> Regardless of whether they contain appeals for attacks, all of these materials are used to generate buy-in for the ideology behind Isis and other groups comprising the global jihad movement. A further problem is that most popular social media and file-sharing companies allow account managers whose identities are unknown to simultaneously use various technologies, such as virtual private networks and specialised browsers such as Tor, to mask their physical locations when active on their sites.

Connecting material available on Tor to the 'ideology behind Isis' is an extreme instance of how the media can link this technology to negative uses and simply ignore the positive aspects. In this example, as well as in the previous ones, Tor is only seen from the perspective of facilitating illegal activities as well as helping criminals hide from authorities, which is not only a biased, but also a vilifying representation of this platform. Thus, this analysis helps conclude that the negative angle of Tor provided by the British press reproduces the concept of hyper-panic, in that media panic (in this case, related to Tor as a technology that enables online anonymity) multiplies moral panic (drugs, paedophilia, terrorism and others).

7.5 Discussion: the Good, the Bad and the Ugly

As this chapter argues, positive and negative perspectives of the Tor Network are a persistent part of the British press representation of this system, reproducing the logic through which academic research approaches this technology (Bartlett, 2015; Hawkins, 2016; Jardine, 2018a; Moore & Rid, 2016; Sui et al., 2015). Opposing good and bad uses and associations is also the way in which British press portray the Deep Web overall, as addressed in Chapters 4 and 5. As a matter of fact, Tor's ambivalence is evident in the media discourse and openly discussed in the articles: there are cases where multiple sides, and of course the contradictions that they impose, ignite a broader debate about privacy-granting technologies.

This analysis compellingly shows, however, that presenting multiple uses of Tor is not necessarily an indication that the article adopts a balanced approach to this technology. Actually, in most instances, the overall argument displays a strongly negative bias towards Tor, even when positive perspectives are mentioned in the article. There are cases, for instance, in which positive

uses are cited ironically, and there are cases in which the hyper-panic surrounding Tor nullifies any positive consequences, such as protecting freedom of speech and personal liberties (Bellare & Rogaway, 2005; Cammaerts, 2013; Dingledine et al., 2004; Grey, 2016; Loesing, 2009; Moore & Rid, 2016). Conversely, criminal uses are acknowledged but belittled in view of the benefit of having a liberation technology available. Thus, while Tor's technological ambivalence is acknowledged by pointing to contrasting uses and associations (Arribas-Ayllon & Bartlett, 2014; Jardine, 2018a), the British press are sharply negative in their representation, applying language and discourse to defend their support or disapproval.

Connecting Tor to negative uses defies the idea that, as the example of other technologies, Tor must be seen in terms of its ambivalence (Schraube, 2009). Its meaning is connected to uses and depends on social, cultural, political and economic contexts, so how can the media simply state that this technology is right or wrong, without adding nuances and embracing its contradictions? Newspaper articles mention genuine uses of Tor, in which personal privacy is protected and freedom of speech and information are assured, and illicit uses, in which criminals hide behind online anonymity. In contrast with what is seen in the discussions about the Deep Web technologies in general and their representation as a threat, British newspapers' coverage of Tor offers positive and negative uses. Ultimately, however, newspapers still choose one or another perspective to argue in favour, and predominantly negative uses are employed. The ambivalence of Tor is there, but polarisation persists. Furthermore, there are examples in which Tor's availability is questioned, or at least seen as a paradox, with the press stating that this technology assures online freedom, which is why the US Government invests in its maintenance, even though it can be used to commit crimes. In a sense, newspapers maintain the same logic that it is more socially acceptable to choose a side than to acknowledge that maybe there is not just one right approach to the topic (Arribas-Ayllon & Bartlett, 2014; Bauman, 1990).

Finally, this research also includes cases that are exclusively against Tor. Ignoring any attempt at unbiased coverage, and trying to show some independence by including positive uses of this system, newspaper articles that focus only on harmful uses clearly reveal the hyper-panic the media generates around this technology. The majority of the negative articles about Tor centre on Silk Road, a crypto market specialising in connecting drug sellers and buyers, but it is not solely

drugs that are associated with Tor, since the most prominent cases allude to sexual violence and terrorism. Overall, Tor is represented in these articles more as a villain than as a technology, because it helps criminals, its main purpose it to conceal identities so people can commit illegal actions, it encourages people to be unscrupulous and so on. The fact that it can save the lives of dissidents in authoritarian regimes or assure accountability in liberal societies, among other positive uses, is completely ignored. Once again, the discussion is not about why people become criminals but why Tor is available for them to commit crimes, as if this were the only objective. This perspective propagates an unnerving circle in which Tor is seen as a threat and not as an ambivalent tool that can be used for positive or negative activities. It only depends on the user's purpose.

Conclusion

The key objective of this research, as initially proposed, was to understand how the British press have represented Deep Web technologies over the course of 17 years, starting with the first publication on the topic retrieved in the sample (2001-2017). After examining 833 articles published by the British newspapers *Daily Mail*, *Daily Mirror*, *Daily Telegraph*, *The Guardian*, *The Times* and *The Sun* – a mix that includes tabloid and quality newspapers with the highest daily reach and multiple political views – through an extensive content analysis, followed by an additional critical discourse analysis specifically about the Tor Network, methods that complement each other to explore multiple angles, it is finally possible to determine the media portrayal of these technologies. In summary, the Deep Web is negatively represented in the British press, which bestow a dimension of darkness and criminality upon these technologies by portraying them as harmful, inexplicable and opaque. Moreover, the media consistently connect the Deep Web to social anxieties, characterising it as undesirable, immoral and illegal. This is achieved through episodic coverage that reinforces negative uses. This consistent association between the Deep Web and criminal and antisocial behaviours promotes a dissociation between the Deep Web and the Web itself: as the imaginary promoted by the British press, the Deep Web is a place for evil undertakings, and the Web is a legitimate and positive space for interaction. Specifically about Tor, the media report on multiple aspects of this system, from the ways in which it can enable civil liberties, to condemning criminals hiding behind technology, which shows that there is an inherent ambivalence connected to the uses of online anonymity, i.e. it is neither completely bad nor completely good. In the next subsection, the conclusions of this thesis are related to the research questions, highlighting the contributions of this work, as well as limitations and directions for future research.

Summary of the Findings

The British press instigate opacity and fear of Deep Web technologies, as well as present a polarised discourse about the Tor Network through the prevalence of negative uses and a

pessimistic approach. The ways in which this is done are related to the answers to the research questions proposed in the *Methodological Framework* and listed below.

RQ1) How do the British press represent the Deep Web?

This thesis shows that Deep Web technologies are portrayed in a sharply negative way by the press. British newspapers make little or no contribution to educating readers on the Deep Web's positive attributes and uses. Instead, the press massively focus on negative connotations while simultaneously vilifying these technologies. Furthermore, British newspapers consistently use negative metaphors to describe these technologies – the term "Dark Web" is greatly adopted by newspapers, while more neutral terms such as "Deep Web" or "Hidden Web" are partially ignored. Moreover, while the academic literature distinguishes between the terms "Dark Web" and "Deep Web," this analysis shows that they are used interchangeably in the British press, proving how newspapers struggle with this concept.

In addition, the hyper-panic concept proposed by this work embraces the idea of a core facilitator of antisocial and criminal behaviours and is responsible for amassing anxiety: a phenomenon in which primary media panic encourages additional secondary moral panic. This is the case for the Deep Web, in that there is panic related to its affordances, especially for allowing online anonymity and protecting users' privacy and against surveillance, which incites several other well-known social fears that the Internet can hide. In addition, there is the panic related to these technologies' opacity, especially because the media exploit a general lack of technical knowledge to spread a superficial and negative rhetoric about new technologies. Finally, the threat is also connected to the purposes of its users, including the misleading idea that criminals are taking over these technologies and that there are no positive uses out there. Consequently, British newspapers address the technical advances that can facilitate illegalities through user and use stereotypes, instead of reflecting social problems that foster inequalities and criminality.

RQ2) What discourse do the British press use to portray the Tor Network?

While the Deep Web is mostly represented in sharply negative ways by the media, thus engendering confusion and fear, critical discourse analysis of articles about positive uses of the Tor Network shows that Tor is also seen as a response to surveillance and censorship practices,

and supporting its use also involves supporting freedom of speech, open access to knowledge, democracy and human dignity, values usually protected by the media. Furthermore, the British press offer a liberation technology point of view based especially on the discussion of issues related to freedoms: criticising state censorship and surveillance is related to freedom of information, discussing privacy issues is related to protecting personal freedoms, human rights and dignity, supporting the right to online anonymity and defending activism are linked to various freedoms, such as expression, speech and information. Even in those cases in which Tor is seen as positive and necessary, however, newspapers twist the discussion and, instead of addressing the problem of state control through surveillance and reflecting on its causes and consequences, the media transfer the burden and the blame to Internet users. As such, Tor is this magical way through which a person can protect him- or herself, and newspapers can educate people on how to use it, but the state will continue acting in this manner, as there is apparently no solution – or, at least, the British press are not willing to help uncover the solution. At the same time, using privacy-granting technologies not only depend on technical knowledge but are also largely stereotyped by the media as negative, which shows how inconsistent the messages promulgated by British newspapers can be. More so, positive uses of Tor rely mainly on coverage by *The Guardian*, which represents 76.4% of the total. This newspaper was at the centre of the Snowden revelations and is considered as willing to investigate the state by scrutinising sensitive issues.

In addition, good and bad views of the Tor Network are a persistent component of the British press's representation of this technology. However, presenting multiple points of view about Tor is not necessarily an indication that the articles adopt a balanced approach to the technology. In most cases, the general argument takes a strongly negative biased approach to Tor, even though positive perspectives are considered. There are cases, for instance, in which positive uses are mentioned ironically, but others where no positive consequences, such as protecting freedom of speech, are cited, thus fermenting the hyper-panic around Tor. Consequently, while a degree of technological ambivalence is acknowledged by pointing to the contrasting uses of Tor, British newspapers still focus sharply on its negative uses, applying language and discourse to defend their contrariety. Although newspaper articles mention legitimate uses of Tor in which personal privacy is protected and freedom of speech and information is assured, as the ambivalence is

there, the polarisation persists: newspapers maintain the same logic that it is more socially acceptable to choose a side even when acknowledging both. Furthermore, Tor's own availability is questioned while public investment in its maintenance are seen as a paradox.

Finally, considering the negative views of Tor as a reason for hyper-panic, most of the articles about it centre on Silk Road, a crypto market specialising in connecting drug sellers and buyers. However, it is not solely drugs that are associated with Tor: the most prominent cases allude to child abuse and terrorism. Overall, Tor is represented in these articles more as a villain than as a technology, in that it helps criminals, its main purpose is to conceal identities so people can commit illegal actions, it encourages people to be unscrupulous and so in. The fact that it can save the lives of dissidents in authoritarian regimes or assure accountability in liberal societies, among other positive uses, is ignored in these cases. Once again, the discussion is not about why people become criminals, but why Tor is available for them to commit crimes, as if this were the only objective. This perspective creates an unnerving circle in which Tor is seen as a threat, a representation that connects privacy-enhancing technologies with the fear of being out of control, which in turn legitimises the culture of surveillance to which contemporary societies are submitted. Specifically about Tor, however, considering that the media present multiple aspects of this system, from discussing the ways in which it can enable civil liberties, to condemning criminals hiding behind technology, this at least shows that there inherent ambivalence is connected to the uses of online anonymity, i.e. it is neither completely bad nor completely good.

RQ3) To what extent do the British press's representation of Deep Web technologies influence the overall imaginary of new media and the Web?

Overall, the emergence of the "Dark Web," a term that in itself is negative, can be contextualised within a broader shift in representations of the Web, from a situation in which it was presented as a myth, as a harbinger of positive change, to a situation in which there is a more nuanced image with positive and negative visions; in fact, undesirable uses are interspersed, normalised and even derided in British press coverage. Although the Internet has reached a stage of maturity in most developed countries, it continues to feed the imaginary of people, because it deals with dreams and imagination. In the case of the Deep Web, in their daily coverage, the

media persistently add to this imaginary a negative dimension of darkness and secrecy, using concepts connected to negative metaphors, showing little effort in providing comprehensive definitions and explanations regarding these technologies and instead favouring language and attributes that deliberately concede opacity.

This thesis argues that the consistent association between the Deep Web and criminal and antisocial behaviours promotes a dissociation between it and the Web itself. There are now two faces of the Web, found in the imaginary promoted by the British press and even in the academic literature (Bartlett, 2015). On the one hand, the Deep Web – more specifically, the Dark Web – is a place for evil minds, common criminals or people that ignore the law and abuse online anonymity through differing levels of misconduct. And on the other hand, the Web is the online haven populated by good people and their legitimate uses, with so many positive spaces for interaction. This separation between concepts according to positive and negative uses shows the struggles of the media in dealing with technological ambivalence. It is clear that the Deep Web can be used for good and bad reasons, in the same way that the Web can be used for good or bad reasons. The difference is that privacy-enhancing technologies can provide online anonymity to anyone, but the Web only offers online anonymity to highly skilled or highly equipped people, for instance states and corporations. In this sense, cyberspace is separated between negative uses (the Deep Web) and positive uses (the Web) instead of being understood as whole and nuanced.

Contributions

This thesis contributes to the Communication and Media Studies, and more broadly to the Social Sciences community, on both an empirical and a theoretical level. The key contributions are summarised as follows.

The Deep Web's Representation

Showing that the British press represent the Deep Web in a sharply negative way, in that they struggle to conceptualise and define these technologies, fills a gap in the academic literature about the overall representation of the Deep Web. There was no previous research showing the

representation of the Deep Web through empirical data before. This study uses content analysis and critical discourse analysis to state that this negative representation not only ascribes opacity to the Deep Web, related to the distrust of its uses and stereotypical users, but it also creates an environment in which using these technologies are morally unacceptable. The choice of attributes, the metaphors and even the sources used to define the Deep Web actively contribute to this negative portrayal.

The Tor Network's Representation

Understanding the representation of the Tor Network by the media also contributes to unveiling the imaginary of this technology, a topic that was lacking research. Analysing how positive and negative uses of Tor are employed by the media leads to the conclusion that this system can be associated with various freedoms, such as expression, speech and information, even though this discourse distracts people from discussions about state control and surveillance. In addition, these multiple arguments are still found in the polarisation of the overall message that questions Tor's availability through a hyper-panic approach.

The Web's Imaginary

This thesis contributes to research on the imaginary of the Web, arguing that the consistent association between the Deep Web and criminal and antisocial behaviours promotes a dissociation between it and the Web in itself. This represents a shift in the Web representation: negative uses are mostly connected to the idea of "the dark side of the Internet" to which the Deep Web is consistently associated. According to the imaginary promoted by the British press, the Deep Web is a place for evil undertakings, and the Web is a legitimate and positive space for interaction. Specifically on the subject of Tor, the media present multiple aspects of this system, from discussing the ways in which it can enable civil liberties, to condemning criminals hiding behind its digital walls, which shows that there is inherent ambivalence connected to the uses of online anonymity, in that it is neither completely bad nor completely good.

Concept of Hyper-Panic

Proposing a new concept as a theoretical contribution to the field of media studies, this thesis compellingly defines and exemplifies the notion of hyper-panic. This concept brings together the ideas of media panic and moral panic and offers a terminology that applies when media panic (in the case of this work, the Deep Web in itself) multiplies moral panic (for instance, anonymity facilitating terrorism, paedophilia and drugs consumption).

Criminalisation of Privacy

Distinct aspects of the British press representation of Deep Web systems as well as its uses and users suggest that media's approach to privacy-enhancing technologies not only creates hyper-panic but also challenges any personal attempt to avoid surveillance. The constructed narrative of the Deep Web is based on distrust, crimes and stereotypes that provide a sense of depravity and risk to the technology and its users. The open and free availability of Tor Network, which can be easily adopted in the context of Western societies, is constantly considered unnecessary or dangerous per se. Moreover, the separation between good and bad uses of the Internet relies on identifying two sides of the Web: the Deep Web offers all the evil possibilities, while the Surface Web is a legitimate and positive space for interaction. The hyper-panic typified by the British media's approach to the Deep Web shows that multiple anxieties are combined to establish a logic of fear. As a whole, aspects identified in the newspapers representation of the Deep Web offer a further consideration: the media discourse proposes more than an overall negative portrayal of privacy-enhancing technologies but a criminalisation of privacy itself. This means that the narrative is constructed in a way that pursuing a more private use of the Internet and defying the surveillance conducted by states and corporations is seen more as an issue than the surveillance per se. Motivations of users that claim for privacy are consistently questioned and undermined. Institutions and groups which fight for fundamental civil rights are silenced in the discussions, with no significance in the news. In summary, British newspapers are reproducing and circulating a very conservative view of privacy in which there are more concerns about risk, safety and the punishment logic than about protecting basic personal liberties.

Target Readership

In terms of audience, this research contributes to scholarly work in at least three fields. For media studies, it presents an extensive examination of British newspaper content and discourse and provides an overall picture of the media's representation of the Deep Web and the Tor Network. For surveillance studies, the discussion in this thesis is related to the representation of one of the most well-known privacy-enhancing technologies, the Tor Network. And for digital studies, this work presents an in-depth analysis of the Deep Web and the Tor Network's meanings and uses, arguing also about the overall imaginary of the Web as well as the portrayal of a new technology.

Challenges and limitations

This research acknowledges challenges and limitations encountered during the course of the analysis. For instance, selecting a large data sample, consisting of 833 newspaper articles from six British newspapers, could be considered an ambitious decision, and indeed this proved itself extremely exhausting and time-consuming. Another point to highlight is the struggle to analyse, organise and present the results of an extensive content analysis, to which was added a critical discourse analysis of 58 publications. Finally, as the primary research was carried out by a non-native English-speaker, who was responsible for an extensive and completely manual coding process, as well as for assuring a critical discourse analysis, language did present some obstacles.

Directions for Future Research

On the matter of how this research can potentially progress, some ideas related to aspects that may be considered in terms of bringing new perspectives to the discussion are as follows:

1. This research concentrates on the British press's representation of Deep Web technologies, so an expected development in this regard would be to conduct the same analysis in the context of different countries, including the Global South, enabling comparisons between different national, linguistic and cultural contexts.
2. Another point is that this research investigates the media representation of Deep Web technologies in the context of the mainstream print media, so there is still the potential

for understanding this representation related to popular culture, such as movies and TV series, or on distinct media platforms, such as television or social media.

3. To unveil the impact of media representation on people's perceptions, a potential work could focus on analysing how the specific readers of these newspapers perceive the Deep Web and to what extent reading negative news can transform attitudes towards these technologies.
4. An exploratory digital ethnography of Tor Network forums could provide valuable insights into the behaviour of Deep Web users.
5. An observation of regular Internet users accessing the Tor Network for the first time could establish what functionalities and uses are directly associated with online anonymity and to what extent users develop negative views or fear related to the technology.
6. Considering the experience with the media's representation of technologies in relation to surveillance studies, another potential development would be to analyse other technologies used for surveillance, for instance the video assistant referee (VAR) in football or CCTV in private homes (used to monitor pets, baby-sitters and others).

References

Abbasi, A., & Chen, H. (2007). Affect intensity analysis of dark web forums. In *ISI 2007: 2007 IEEE Intelligence and Security Informatics* (pp. 282-288). https://doi.org/10.1109/isi.2007.379486

Ahmed, S., & Matthes, J. (2017). Media representation of Muslims and Islam from 2000 to 2015: A meta-analysis. *International Communication Gazette*, 79(3), 219-244. https://doi.org/10.1177/1748048516656305

Aiken, M. (2016). *The Cyber Effect*. John Murray (Publishers).

Al-Rawi, A. (2019). Islamic State in Iraq and Syria's standardized media and jihadist nation-state building efforts. *Communication and the Public*, 4(3), 224-238. https://doi.org/10.1177/2057047319853323

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*. https://doi.org/10.5210/fm.v13i3.2142

Aldridge, J. (2019). Does online anonymity boost illegal market trading? *Media, Culture & Society*, 41(4), 578-583. https://doi.org/10.1177/0163443719842075

Aldridge, J., & Décary-Hétu, D. (2014). Not an 'eBay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *SSRN*. http://dx.doi.org/10.2139/ssrn.2436643

Altman, I. (1977), Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33: 66-84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

Andersen, J. (2018). Archiving, ordering, and searching: search engines, algorithms, databases, and deep mediatization. *Media, Culture & Society*, 40(8), 1135-1150. https://doi.org/10.1177/0163443718754652

Anti-social Behaviour, Crime and Policing Act 2014 (c.12) (UK). Retrieved 10th January 2020, from the UK Government website: http://www.legislation.gov.uk/ukpga/2014/12/pdfs/ukpga_20140012_en.pdf

Antonopoulos, G. A., & Hall, A. (2016). 'Gain with no pain': Anabolic-androgenic steroids trafficking in the UK. *European Journal of Criminology*, 13(6), 696-713. https://doi.org/10.1177/1477370816633261

Armon, R. (2017). Radio Sensors and Electric Storms: Scientific Metaphors in Media Talks. *Science Communication*, 39(4), 443-465. https://doi.org/10.1177/1075547017718362

Arribas-Ayllon, M., & Bartlett, A. (2014). Sociological Ambivalence and the Order of Scientific Knowledge. *Sociology*, 48(2), 335-351. https://doi.org/10.1177/0038038513477937

Ashby, W. R. (1957). *An Introduction to Cybernetics*. Chapman & Hall Ltd.

Baek, S., Seo, S.-H., & Kim, S. (2016). Preserving Patient's Anonymity for Mobile Healthcare System in IoT Environment. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/155014772171642

Baker, V. (2015). Don't judge a reader by their book: The danger of owning or reading certain texts. *Index on Censorship*, 44(4), 118-120. https://doi.org/10.1177/0306422015622948

Bakken, S. A., Moeller, K., & Sandberg, S. (2018). Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology*, 15(4), 442-460. https://doi.org/10.1177/1477370817749177

Bancroft, A., Squirrell, T., Zaunseder, A., & Rafanell, I. (2019). Producing Trust Among Illicit Actors: A Techno-Social Approach to an Online Illicit Market. *Sociological Research Online*. https://doi.org/10.1177/1360780419881158

Banks, M. (2005). Spaces of (in)security: Media and fear of crime in a local context. *Crime, Media, Culture*, 1(2), 169-187. https://doi.org/10.1177/1741659005054020

Barabási, A. L. (2002). *Linked: The New Science Of Networks*. Perseus Publishing.

Barney, D., Coleman, G., Ross, C., Sterne, J., Tembeck, T. (2016). *The Participatory Condition in the Digital Age*. University of Minnesota Press.

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research*, 16(6), 701-719. https://doi.org/10.1177/1468794116648766

Bartlett, J. (2015). *The Dark Net*. Windmill Books.

Bartlett, J., & Krasodomski-Jones, A. (2015). *Online Anonymity, Islamic State and Surveillance*. Demos.

Bauman, Z. (1990). Modernity and Ambivalence. *Theory, Culture & Society*, 7, 143-169.

Beccaria, C. B. (1872). *An Essay on Crimes and Punishments*. W.C. Little & Co.

Bednarek, M., & Caple, H. (2014). Why do news values matter? Towards a new methodological framework for analysing news discourse in Critical Discourse Analysis and beyond. *Discourse & Society*, 25(2), 135-158. https://doi.org/10.1177/0957926513516041

Bellare, M.; & Rogaway, P. (2005). *Introduction to Modern Cryptography*.

Bentham, J. (1995). *The Panopticon Writings*. Verso.

Berg, M. (1998). The Politics of Technology: On Bringing Social Theory into Technological Design. *Science, Technology, & Human Values*, 23(4), 456-490. https://doi.org/10.1177/016224399802300406

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing*, 7(1). http://dx.doi.org/10.3998/3336451.0007.104

Berners-Lee, T. (2000). *Weaving the Web: The Original Design of the World Wide Web by its inventor*. HarperCollins Publishers.

Bignell, J. (2002). *Media semiotics: an introduction*. Manchester University Press.

Bijker, W. E. (1995). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. The MIT Press.

Bishop, J. P. (2019). Ageing and the Technological Imaginary: Living and Dying in the Age of Perpetual Innovation. *Studies in Christian Ethics*, 32(1), 20-35. https://doi.org/10.1177/0953946818807462

Bjerg, O. (2016). How is Bitcoin Money? *Theory, Culture & Society*, 33(1), 53-72. https://doi.org/10.1177/0263276415619015

Bleakley, P. (2019). Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks. *The Police Journal*, 92(3), 221-236. https://doi.org/10.1177/0032258X18801409

Bolton, N. (1997). *Concept Formation*. Pergamon Press.

Bory, P., Benecchi, E., & Balbi, G. (2016). How the Web was told: Continuity and change in the founding fathers' narratives on the origins of the World Wide Web. *New Media & Society*, 18(7), 1066-1087. https://doi.org/10.1177/1461444816643788

Bourdieu, P. (1998). *On Television*. The New Press.

Bradbury, D. (2014). Unveiling the dark web. *Network Security*, 2014(4), 14-17. https://doi.org/10.1016/S1353-4858(14)70042-X.

Branum, J., & Charteris-Black, J. (2015). The Edward Snowden affair: A corpus study of the British press. *Discourse & Communication*, 9(2), 199-220. https://doi.org/10.1177/1750481314568544

Branum, J., & Charteris-Black, J. (2015). The Edward Snowden affair: A corpus study of the British press. Discourse & Communication, 9(2), 199-220. https://doi.org/10.1177/1750481314568544

Brown, J. D., Bybee, C. R., Wearden, S. T., & Straughan, D. M. (1987). Invisible Power: Newspaper News Sources and the Limits of Diversity. *Journalism Quarterly*, 64(1), 45-54. https://doi.org/10.1177/107769908706400106

Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal*, 89(4), 327-339. https://doi.org/10.1177/0032258X16658927

Brummette, J., DiStaso, M., Vafeiadis, M., & Messner, M. (2018). Read All About It: The Politicization of "Fake News" on Twitter. *Journalism & Mass Communication Quarterly*, 95(2), 497-517. https://doi.org/10.1177/1077699018769906

Brunton, F. (2013). *Spam: A Shadow History of The Internet*. The MIT Press.

Bucher, T. (2019). Bad Guys and Bag Ladies: On the Politics of Polemics and the Promise of Ambivalence. *Social Media + Society*. https://doi.org/10.1177/2056305119856705

Burgoon, J. K. (1982) Privacy and Communication. *Annals of the International Communication Association*, 6(1), 206-249. https://doi.org/10.1080/23808985.1982.11678499

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*. https://doi.org/10.1177/2053951715622512

Cammaerts, B. (2013). Networked Resistance: The Case of WikiLeaks. *Journal of Computer-Mediated Communication*, 18(4), 420-436, https://doi.org/10.1111/jcc4.12024

Cammaerts, B. (2015). Technologies of self-mediation: affordances and constraints of social media for protest movements. In Uldam, J.; & Vestergaard, A. (pp. 97-110). *Civic Engagement and Social Media: Political Participation Beyond Protest*. Palgrave Macmillan.

Campbell, E. (2016). Policing paedophilia: Assembling bodies, spaces and things. *Crime, Media, Culture*, 12(3), 345-365. https://doi.org/10.1177/1741659015623598

Carpentier, N. (2011). *Media and Participation*. Gutenberg Press.

Castells, M. (2010). *The Rise of the Network Society*. Wiley-Blackwell.

Cavender, G. (2004). Media and Crime Policy: A Reconsideration of David Garland's The Culture of Control. *Punishment & Society*, 6(3), 335-348. https://doi.org/10.1177/1462474504043636

Chadee, D., & Ditton, J. (2005). Fear of crime and the media: Assessing the lack of relationship. *Crime, Media, Culture*, 1(3): 322-32. https://doi.org/10.1177/1741659005057644

Chadwick, A., Vaccari, C., & O'Loughlin, B. (2018). Do tabloids poison the well of social media? Explaining democratically dysfunctional news sharing. *New Media & Society*, 20(11), 4255-4274. https://doi.org/10.1177/1461444818769689

Chen, H.-T. (2018). Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist*, 62(10), 1392-1412. https://doi.org/10.1177/0002764218792691

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008), Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*, 59, 1347-1359. https://doi.org/10.1002/asi.20838

Chimombo, M. P. F., & Roseberry, R. L. (1998). *The Power of Discourse*. Laurence Erlbaum Associates Publishers.

Chopra, S., & Dexter, S. D. (2007). *Decoding Liberation: The Promise of Free and Open Source Software*. Routledge.

Chouliaraki, L. (2010). Self-mediation: new media and citizenship. *Critical Discourse Studies*, 7(4), 227-232. https://doi.org/10.1080/17405904.2010.511824

Christidou, V., Dimopoulos, K., & Koulaidis, V. (2004). Constructing social representations of science and technology: the role of metaphors in the press and the popular scientific magazines. *Public Understanding of Science*, 13(4), 347-362. http://doi.org/10.1177/0963662504044108

Coddington, M. (2014). Defending judgment and context in 'original reporting': Journalists' construction of newswork in a networked age. *Journalism*, 15(6), 678–695. https://doi.org/10.1177/1464884913501244

Cohen, S. (2011). Folk Devils and Moral Panics. Routledge Classics.

Cole, P. (2015). A changing of The Guardian. *British Journalism Review*, 26(2), 19-28. https://doi.org/10.1177/0956474815589541

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso.

Coleman, G. (2019). How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing? *Media, Culture & Society*, 41(4), 565-571. https://doi.org/10.1177/0163443719843867

Collins, V. E., Farrell, A. L., McKee, J. R., Martin, F. A., & Monk-Turner, E. (2011). The State of Coverage: The Media's Representation of International Issues and State Crime. *International Criminal Justice Review*, 21(1), 5-21. https://doi.org/10.1177/1057567711398306

Conboy, M. (2006). *Tabloid Britain: Constructing a Community through Language*. Routledge.

Contractor, A. A., Weiss, N. H., & Elhai, J. D. (2019). Examination of the Relation Between PTSD Symptoms, Smartphone Feature Uses, and Problematic Smartphone Use. *Social Science Computer Review*, 37(3), 385-403. https://doi.org/10.1177/0894439318770745

Cottle, S. (2009). Journalism studies: coming of (global) age? *Journalism*, 10(3), 309-311. http://doi.org/10.1177/1464884909102573

Crawford, S. P. (2007). Internet Think. *Journal on Telecommunications and High Technology Law*, 467-486. https://ssrn.com/abstract=962596

Cross, S. (2014). Mad and bad media: Populism and pathology in the British tabloids. *European Journal of Communication*, 29(2), 204-217. https://doi.org/10.1177/0267323113516734

de Vries, P., & Schinkel, W. (2019). Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms. *Big Data & Society*. https://doi.org/10.1177/2053951719851532

Deacon, D. (2007). Yesterday's papers and today's technology: digital newspaper archives and 'push button' content analysis. *European Journal of Communication*, 22 (1), 5-25. https://doi.org/10.1177/0267323107073743

Deacon, D., Pickering, M., Golding, P., & Murdock, G. (2007). *Researching Communications: A Practical Guide to Methods in Media and Cultural Analysis*. Bloomsbury.

Décary-Hétu, D., Mousseau, V., & Vidal, S. (2018). Six Years Later: Analyzing Online Black Markets Involved in Herbal Cannabis Drug Dealing in the United States. *Contemporary Drug Problems*, 45(4), 366–381. https://doi.org/10.1177/0091450918797355

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, 59, 3-7.

Demant, J., Munksgaard, R., Décary-Hétu, D., & Aldridge, J. (2018). Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime. *International Criminal Justice Review*, 28(3), 255-274. https://doi.org/10.1177/1057567718769719

Devine, J.; & Egger-Sider, F. (2014). *Going Beyond Google Again: Strategies for Using and Teaching the Invisible Web*. Neal-Schuman Publishers.

Diamond, L. (2012). Liberation Technology. In Diamond, L., & Plattner, M. F. *Liberation Technology: Social Media and the Struggle for Democracy* (pp. 3-17). The Johns Hopkins University Press.

Diffie, W.; & Landau, S. (2007). *Privacy on the line*. The MIT Press.

Dinev, T.; Hart, P.; & Mullen, M. R. (2008). Internet Privacy Concerns and Beliefs about Government Surveillance: An Empirical Investigation. *Journal of Strategic Information Systems*, 17, 214-233. https://doi.org/10.1016/j.jsis.2007.09.002

Dingledine, R. (2010). Tools of the Trade. *Index on Censorship*, 39(1), 127-137. https://doi.org/10.1177/0306422010363345

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. *SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium*, 13.

Doğu, B. (2017). Turkey's news media landscape in Twitter: Mapping interconnections among diversity. *Journalism*. https://doi.org/10.1177/1464884917713791

Dourish, Paul. (2015). *Protocols, packets, and proximity*. In Parks, Lisa; Starosielski, Nicole. Signal Traffic: Critical Studies of Media Infrastructures. University of Illinois Press.

Doyle, T. (2018). Privacy, obfuscation, and propertization. *IFLA Journal*, 44(3), 229-239. https://doi.org/10.1177/0340035218778054

Drotner, K. (1999). Dangerous Media? Panic Discourses and Dilemmas of Modernity, *Paedagogica Historica*, 35(3), 593-619, https://doi.org/10.1080/0030923990350303

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal*, 72(4), 538-562. https://doi.org/10.1177/0020702017741909

Dupont, B., Côté, A.-M., Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World." *American Behavioral Scientist*, 61(11), 1219-1243. https://doi.org/10.1177/0002764217734263

Durham, M. G, & Kellner, D. M. (2006). *Media and Cultural Studies*. Blackwell Publishing.

Ellsworth, J. H., & Ellsworth, M. V. (1994). *The Internet Business Book*. John Wiley & Sons, Inc.

Fairclough, N. (2004). *Analysing Discourse: Textual analysis for social research*. Routledge.

Feenberg, A. (1990). The ambivalence of technology. *Sociological Perspectives*, 33(1), 35-50.

Ferguson, R.-H. (2017). Offline 'stranger' and online lurker: methods for an ethnography of illicit transactions on the darknet. *Qualitative Research*, 17(6), 683-698. https://doi.org/10.1177/1468794117718894

Fink, L., & Hyatt, M. P. (1978). Drug use and criminal behaviour. *Journal of Drug Education*, 8(2), 139-149. http://doi.org/10.2190/L6U3-NURL-C67V-L0QV

Flichy, P. (2007). *The Internet Imaginaire*. MIT Press.

Floridi, L. (2014). *The Fourth Revolution*. Oxford University Press.

Forceville, C. J., & Renckens, T. (2013). The good is light and bad is dark: Metaphor in feature films. *Metaphor and the Social World*, 3(2), 160-179. https://doi.org/10.1075/msw.3.2.03for

Foucault, M. (1995). *Discipline & Punish*. Vintage Books.

Fu, T., Abbasi, A., & Chen, H. (2010). A focused crawler for Dark Web forums. *Journal of the American Society for Information Science and Technology*, 61(6), 1213-1231. https://doi.org/10.1002/asi.21323

Furedi, F. (2016). Moral Panic and Reading: Early Elite Anxieties About the Media Effect. *Cultural Sociology*, 10(4), 523-537. https://doi.org/10.1177/1749975515626953

Fürsich, E. (2010). Media and the representation of Others First. *International Social Science Journal*, 61(1999), 113-130. https://doi.org/10.1111/j.1468-2451.2010.01751.x

Gandy, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press, Inc.

Gangadharan, S. P. (2017). The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. *New Media & Society*, 19(4), 597–615. https://doi.org/10.1177/1461444815614053

Garcia-Rivadulla, S. (2016). Personalization vs. privacy: An inevitable trade-off? *IFLA Journal*, 42(3), 227-238. https://doi.org/10.1177/0340035216662890

https://doi.org/10.1177/1741659007087270

Gehl, R. W. (2015). The Case for Alternative Social Media. *Social Media + Society*. https://doi.org/10.1177/2056305115604338

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 18(7), 1219-1235. https://doi.org/10.1177/1461444814554900

Gehl, R., & McKelvey, F. (2019). Bugging out: darknets as parasites of large-scale media objects. *Media, Culture & Society*, 41(2), 219-235. https://doi.org/10.1177/0163443718818379

Gibson, J. J. (1979). *The ecological approach to visual perception*. Eribaum Associates Publishers.

Gillespie, T. (2012). The Relevance of Algorithms. In Gillespie, T., Boczkowski, P., & Foot, K. *Media Technologies*. The MIT Press.

Gitelman, L., & Pingree, G. B. (2003). *New Media, 1740-1915*. The MIT Press.

Goffey, A. (2008). Algorithm. In Fuller, M. (pp. 15-17). *Software Studies: A Lexicon*. The MIT Press.

Graham, R., & Pitman, B. (2018). Freedom in the wilderness: A study of a Darknet space. *Convergence*. https://doi.org/10.1177/1354856518806636

Gray, M. (2003). Urban Surveillance and Panopticism: Will We Recognize The Facial Recognition Society? *Surveillance & Society*, 1(3), 314-330. https://doi.org/10.24908/ss.v1i3.3343

Greenberg, K. J. (2016). Counter-Radicalization via the Internet. *AAPSS*, 668, 165-179.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA & the Surveillance State*. Penguin Books.

Grey, S. (2016). Is your secret safe with me? Difficulties of protecting sources amid mass surveillance. *Index on Censorship*, 45(2), 58-61. https://doi.org/10.1177/0306422016657028

Guitton, C. (2013). A review of the available content on Tor hidden services: The case against further development. *Computers in Human Behavior*, 29(6), 2805-2815. https://doi.org/10.1016/j.chb.2013.07.031

Habermas, J. (2006). The Public Sphere: An Encyclopedia Article. In Durham, M. G, & Kellner, D. M. (Ed). *Media and Cultural Studies* (pp. 73-78). Blackwell Publishing.

Haggerty, K. D., & Ericson, R. V. (2000). The Surveillant Assemblage. *British Journal of Sociology*, 51(4), 605-622.

Haines, A., & Wells, H. (2012). Persecution or protection? Understanding the differential public response to two road-based surveillance systems. *Criminology & Criminal Justice*, 12(3), 257-273. https://doi.org/10.1177/1748895811431848

Hall, S. (2013). *Representation: Cultural Representations and Signifying Practices*. Sage Publications.

Hanitzsch, T., Löffelholz, M., & Weaver, D. H. (2005). Building a home for the study of journalism: ICA creates a Journalism Studies Interest Group. *Journalism*, 6(1), 107-115.

Haran, J., & Kitzinger, J. (2009). Modest witnessing and managing the boundaries between science and the media: A case study of breakthrough and scandal. *Public Understanding of Science*, 18(6), 634-652. https://doi.org/10.1177/0963662509338324

Harper, C. A., & Hogue, T. E. (2015). The Emotional Representation of Sexual Crime in the National British Press. *Journal of Language and Social Psychology*, 34(1), 3-24. https://doi.org/10.1177/0261927X14544474

Hartley, J. (2000). Communicative democracy in a redactional society: the future of journalism studies. *Journalism*, 1(1), 39-48.

Hasinoff, A. A. (2013). Sexting as media production: Rethinking social media and sexuality. *New Media & Society*, 15(4), 449-465. https://doi.org/10.1177/1461444812459171

Hawkins, B. (2016). Under the Ocean of the Internet – The Deep Web*. SANS Institute InfoSec Reading Room*.

He, Y., Xin, D., Ganti, V., Rajaraman, S., & Shah, N. (2013). Crawling deep web entity pages. In *Proceedings of the sixth ACM international conference on Web search and data mining* (WSDM '13). ACM, New York, NY, USA, 355-364. https://doi.org/10.1145/2433396.2433442

Hickman, M. (1982). Crime in the streets — A moral panic: Understanding "get tough" policies in the criminal justice system. *American Journal of Criminal Justice*, 7(1), 7-22. https://doi.org/10.1007/BF03373788

Hoang, N. P., & Pishva, D. (2014). Anonymous communication and its importance in social networking. *16th International Conference on Advanced Communication Technology*, Pyeongchang, 34-39. https://doi.org/10.1109/ICACT.2014.6778917

Hoffman, L. H., & Slater, M. D. (2007). Evaluating public discourse in newspaper opinion articles: Values-framing and integrative complexity in substance and health policy issues. *Journalism and Mass Communication Quarterly*, 84(1), 58-74. https://doi.org/10.1177/107769900708400105

Hope, A. (2009). CCTV, School Surveillance and Social Control. *British Educational Research Journal*, 35:6, 891-907. https://doi.org/10.1080/01411920902834233

Hossain, M. S. (2015). Social Media and Terrorism: Threats and Challenges to the Modern Era. *South Asian Survey*, 22(2), 136-155. https://doi.org/10.1177/0971523117753280

Hsieh, Y. P. (2012). Online social networking skills: The social affordances approach to digital inequality. *First Monday*, 17(4). https://ojphi.org/ojs/index.php/fm/rt/printerFriendly/3893/3192

Hurley, Z. (2019). Why I No Longer Believe Social Media Is Cool… *Social Media + Society*. https://doi.org/10.1177/2056305119849495

Imre, I., Pjesivac, I., & Luther, C. A. (2016). Governmental control of the Internet and WikiLeaks: How does the press in four countries discuss freedom of expression*? International Communication Gazette*, 78(5), 385-410. https://doi.org/10.1177/1748048516640203

Information Commissioner's Office. (2019). Information Rights Research. Retrieved 10th January 2020, from the Information Commissioner's Office website: https://ico.org.uk/about-the-ico/our-information/research-and-reports/information-rights-research

Iosifidis, P., & Andrews, L. (2019). Regulating the internet intermediaries in a post-truth world: Beyond media policy? *International Communication Gazette*. https://doi.org/10.1177/1748048519828595

Iyengar, S. (1990). Framing Responsibility for Political Issues: The Case of Poverty. Political Behavior, 12(1), 19-40. http://links.jstor.org/sici?sici=0190-9320%28199003%2912%3A1%3C19%3AFRFPIT%3E2.0.CO%3B2-V

Jaeger, C. (2015). *Deep Web Secrecy and Security*. Kindle edition.

Jardine, E. (2018a). Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media & Society*, 20(8), 2824-2843. https://doi.org/10.1177/1461444817733134

Jardine, E. (2018b). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society*, 20(2), 435-452. https://doi.org/10.1177/1461444816639976

Jones, P. (1998). The Technology Is Not the Cultural Form?: Raymond Williams's Sociological Critique of Marshall McLuhan. *Canadian Journal of Communication*, 23(4).

Jordan, T. (2008). *Digital Media and Technological Determinism*. Polity Press.

Jordan, T. (2009). Hacking and power: Social and technological determinism in the digital age. *First Monday*, Volume 14, Number 7. https://doi.org/10.5210/fm.v14i7.2417

Jordan, T. (2017). A genealogy of hacking. *Convergence*, 23(5), 528-544.

Jordan, T. (2019). Does online anonymity undermine the sense of personal responsibility? *Media, Culture & Society*, 41(4), 572-577. https://doi.org/10.1177/0163443719842073

Kane, A. M. (2015). A revocable anonymity in Tor. *Cryptology ePrint Archive*. https://eprint.iacr.org/2015/215.pdf

Kang, K., Choo, J., & Kim, Y. (2019). Whose Opinion Matters? Analyzing Relationships Between Bitcoin Prices and User Groups in Online Community. *Social Science Computer Review*. https://doi.org/10.1177/0894439319840716

Kavanagh, D., Miscione, G., & Ennis, P. (2019). The Bitcoin game: Ethno-resonance as method. *Organization*, 26(4), 517-536. https://doi.org/10.1177/1350508419828567

Kelley, D. R. (1996). On the Margins of Begriffsgeschichte. In Lehmann, H., & Richter, M. *The meaning of historical terms and concepts: New studies on Begriffsgeschichte*. German Historical Institute.

Kendrick, T. (2007). The winning mindset: Effective competitive intelligence research on the internet. *Business Information Review*, 24(4), 228-235. https://doi.org/10.1177/0266382107084890

Kennedy, H. (2006). Beyond anonymity, or future directions for internet identity research. *New Media & Society*, 8(6), 859-876. https://doi.org/10.1177/1461444806069641

Kethineni, S., & Cao, Y. (2019). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*. https://doi.org/10.1177/1057567719827051

Khare, R., An, Y., & Song, I.-Y. (2010). Understanding deep web search interfaces: a survey. *SIGMOD Rec*. 39(1), 33-40. https://doi.org/10.1145/1860702.1860708

Kidd, J. (2016). *Representation*. Routledge.

Kolko, B., Nakamura, L., & Rodman, G. (2013) *Race in Cyberspace*. Routledge.

Koselleck, R. (2002). *The Practice of Conceptual History: Timing History, Spacing Concepts*. Stanford University Press.

Koselleck, R. (2004). *Future Past: On the Semantics of Historical Time*. Columbia University Press.

Krippendorff, K. (2013). *Content Analysis: An Introduction to Its Methodology*. Sage Publications.

Kutscher, N., & Kreß, L.-M. (2018). The Ambivalent Potentials of Social Media Use by Unaccompanied Minor Refugees. *Social Media + Society*. https://doi.org/10.1177/2056305118764438

Ladegaard, I. (2018). Instantly Hooked? Freebies and Samples of Opioids, Cannabis, MDMA, and Other Drugs in an Illicit E-Commerce Market. *Journal of Drug Issues*, 48(2), 226-245. https://doi.org/10.1177/0022042617746975

Ladegaard, I. (2019). "I Pray That We Will Find a Way to Carry on This Dream": How a Law Enforcement Crackdown United an Online Community. *Critical Sociology*, 45(4-5), 631-646. https://doi.org/10.1177/0896920517735670

Lakoff, G., & Johnson, M. (1980). *Metaphors We Live By*. University of Chicago Press.

Landau, S. (2017). *Listening In: Cybersecurity in an Insecure Age*. Yale University Press.

Lane, B. R., Lacey, D., Stanton, N. A., Matthews, A., & Salmon, P. M. (2018). The Dark Side Of The Net: Event Analysis Of Systemic Teamwork (East) Applied To Illicit Trading On A Darknet Market. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), 282-286. https://doi.org/10.1177/1541931218621065

Langer, S. K. (1954). *Philosophy in a New Key: A Study in the Symbolism of Reason, Rite, and Art*. The New American Library.

Larsson, S., Svensson, M., & Kaminski, M. de. (2013). Online piracy, anonymity and social change: Innovation through deviance. *Convergence*, 19(1), 95-114. https://doi.org/10.1177/1354856512456789

Lashmar, P. (2013). Urinal or conduit? Institutional information flow between the UK intelligence services and the news media. *Journalism*, 14(8), 1024-1040. https://doi.org/10.1177/1464884912472139

Latimer, P., & Duffy, M. (2019). Deconstructing Digital Currency and Its Risks: Why ASIC Must Rise to the Regulatory Challenge. *Federal Law Review*, 47(1), 121-150. https://doi.org/10.1177/0067205X18816237

Lee, F. L. F. (2016). Impact of social media on opinion polarization in varying times. *Communication and the Public*, 1(1), 56-71. https://doi.org/10.1177/2057047315617763

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet. *SIGCOMM Comput. Commun. Rev.* 39(5), 22-31. http://dx.doi.org/10.1145/1629607.1629613

Lewis, J., & Hunt, J. (2011). Press coverage of the UK military budget: 1987 to 2009. *Media, War & Conflict*, 4(2), 162-184. https://doi.org/10.1177/1750635211406012

Lianos, M. (2003). Social Control after Foucault. *Surveillance & Society*, 1(3), 412-430.

Lim, S. S. (2013). On mobile communication and youth "deviance": Beyond moral, media and mobile panics. *Mobile Media & Communication*, 1(1), 96-101. https://doi.org/10.1177/2050157912459503

Lindtner, S. (2014). Hackerspaces and the Internet of Things in China: How makers are reinventing industrial production, innovation, and the self. *China Information*, 28(2), 145-167. https://doi.org/10.1177/0920203X14529881

Lippert, R. K., & Walby, K. (2016). Governing Through Privacy: Authoritarian Liberalism, Law, and Privacy Knowledge. *Law, Culture and the Humanities*, 12(2), 329-352. https://doi.org/10.1177/1743872113478530

Liu, F. (2011). The norm of the 'good' netizen and the construction of the 'proper' wired self: The case of Chinese urban youth. *New Media & Society*, 13(1), 7-22. https://doi.org/10.1177/1461444809360701

Liu, W., Meng, X., & Meng, W. (2010). ViDE: A Vision-Based Approach for Deep Web Data Extraction. *IEEE Transactions on Knowledge and Data Engineering*, 22(3), 447-460. https://doi.org/10.1109/TKDE.2009.109

Locke, S. (2005). Fantastically reasonable: ambivalence in the representation of science and technology in super-hero comics. *Public Understanding of Science*, 14(1), 25-46. https://doi.org/10.1177/0963662505048197

Loesing, K. (2009) Measuring the Tor network from public directory information. In *Proceedings of the 4th Hot Topics in Privacy Enhancing Technologies, HotPETS'11*, Seattle, WA, USA, August 2009. Springer-Verlag.

Loocke, P. V. (1999). *The Nature of Concepts*. Routledge.

Lorenzo-Dus, N., & Di Cristofaro, M. (2018). 'I know this whole market is based on the trust you put in me and I don't take that lightly': Trust, community and discourse in crypto-drug markets. *Discourse & Communication*, 12(6), 608-626. https://doi.org/10.1177/1750481318771429

Lu, Y., He, H., Zhao, H., Meng, W., & Yu, C. (2007). Annotating Structured Data of the Deep Web. In 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, 2007, 376-385. https://doi.org/10.1109/ICDE.2007.367883

Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the Limits of Technology's Impact on Police Effectiveness. *Police Quarterly*, 20(2), 135-163. https://doi.org/10.1177/1098611116667279

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Polity Press.

Lyon, D. (2009). Surveillance, Power and Everyday Life. In Avgerou, C., Mansell, R., Quah, D., & Silverstone, R. *Oxford Handbook of Information and Communication Technologies*. Oxford University Press.

Lyon, D. (2015). *Surveillance After Snowden*. Polity Press.

Lyon, D. (2018). *The Culture of Surveillance*. Polity Press.

MacKenzie, D., & Wajcman, J. (1999). *The social shaping of technology*. Open University Press.

Mackey, T. K. (2018). Opioids and the Internet: Convergence of Technology and Policy to Address the Illicit Online Sales of Opioids. *Health Services Insights*. https://doi.org/10.1177/1178632918800995

Macnish, K. (2012). Unblinking Eyes: The Ethics of Automating Surveillance. *Ethics and Information Technology*, 14(2), 151-167. https://doi.org/10.1007/s10676-012-9291-0

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2015). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' *Information, Communication & Society*, 19(1), 111-126, https://doi.org/10.1080/1369118X.2015.1093531

Madhavan, J., Afanasiev, L., Antova, L., & Halevy, A. (2009). Harnessing the Deep Web: present and future. *4th Biennial Conference on Innovative Data Systems Research (CIDR 2009)*, Asilomar, CA, USA. https://hdl.handle.net/11245/1.320590

Madhavan, J., Ko, D., Kot, Ł., Ganapathy, V., Rasmussen, A., & Halevy, A. (2008). Google's Deep Web crawl. *Proc. VLDB Endow*. 1(2), 1241-1252. http://dx.doi.org/10.14778/1454159.1454163

Magdy, S. (2016). A safe space for terrorists. *British Journalism Review*, 27(4), 23-28. https://doi.org/10.1177/0956474816681736

Mager, A. (2017). Search engine imaginary: Visions and values in the co-production of search technology and Europe. *Social Studies of Science*, 47(2), 240-262. https://doi.org/10.1177/0306312716671433

Malbreil, X. (2007). About the internet imaginary and its evolution. *Texto Digital*, 3(1). https://doi.org/10.5007/%x

Manovich, L. (2002). *The Language of New Media*. The MIT Press.

Mansell, R. (2012*). Imagining the Internet: Communication, Innovation, and Governance*. Oxford University Press.

Martin, C. (2012). Video Games, Identity, and the Constellation of Information. Bulletin of Science, *Technology & Society*, 32(5), 384-392. https://doi.org/10.1177/0270467612463797

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket.' *Criminology & Criminal Justice*, 14(3), 351-367. https://doi.org/10.1177/1748895813505234

Marx, K. (1964). *The Communist Manifesto*. Monthly Review Press.

Mason, P. (2006). Lies, distortion and what doesn't work: Monitoring prison stories in the British media. *Crime, Media, Culture*, 2(3), 251-267. https://doi.org/10.1177/1741659006069558

Massanari, A. (2017). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society*, 19(3), 329-346. https://doi.org/10.1177/1461444815608807

Matthewman, S. (2011). *Technology and Social Theory*. Palgrave Macmillan.

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008) Shining Light in Dark Places: Understanding the Tor Network. In: Borisov, N., & Goldberg, I. Privacy Enhancing Technologies. PETS 2008. *Lecture Notes in Computer Science*, 5134. https://doi.org/10.1007/978-3-540-70630-4_5

McGregor, S. C. (2019). Social media as public opinion: How journalists use social media to represent public opinion. *Journalism*, 20(8), 1070-1086. https://doi.org/10.1177/1464884919845458

McLeod, P. L. (2011). Effects of Anonymity and Social Comparison of Rewards on Computer-Mediated Group Brainstorming. *Small Group Research*, 42(4), 475-503. https://doi.org/10.1177/1046496410397381

McLuhan, M. (1964) *Understanding Media: The Extensions of Man*. The MIT Press.

McRobbie, A., & Thornton, S. L. (1995). Rethinking 'Moral Panic' for Multi-Mediated Social Worlds. *The British Journal of Sociology*, 46(4), 559-574. https://www.jstor.org/stable/591571

Melton, J. V. H. (1996). Otto Brunner and the Ideological Origins of Begriffsgeschichte. In: Lehmann, H., & Richter, M. *The meaning of historical terms and concepts: New studies on Begriffsgeschichte*. German Historical Institute.

Menke, M., & Schwarzenegger, C. (2019). On the relativity of old and new media: A lifeworld perspective. *Convergence*, 25(4), 657-672. https://doi.org/10.1177/1354856519834480

Merkley, E. (2019). Partisan Bias in Economic News Content: New Evidence. *American Politics Research*, 47(6), 1303-1323. https://doi.org/10.1177/1532673X18821954

Miller, J. (2014). The fourth screen: Mediatization and the smartphone. *Mobile Media & Communication*, 2(2), 209-226. https://doi.org/10.1177/2050157914521412

Miller, V. (2011). *Understanding Digital Culture*. Sage Publications.

Minárik, T., & Osula, A.-M. Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. *Computer Law & Security Review*, 32(1), 111-127. https://doi.org/10.1016/j.clsr.2015.12.002

Moeller, K., Munksgaard, R., & Demant, J. (2017). Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs. *American Behavioral Scientist*, 61(11), 1427-1450. https://doi.org/10.1177/0002764217734269

Mommsen, T. (1942). Petrarch's Conception of the 'Dark Ages.' *Speculum*, 17(2), 226-242. https://doi.org/10.2307/2856364

Moore, D., & Rid, T. (2016) Cryptopolitik and the Darknet. *Survival*, 58(1), 7-38. https://doi.org/10.1080/00396338.2016.1142085

Moore, R. C. (2006). Ambivalence to Technology in Jeunet's Le Fabuleux Destin d'Amélie Poulain. *Bulletin of Science, Technology & Society*, 26(1), 9-19. https://doi.org/10.1177/0270467605284341

Mörch, C.-M., Côté, L.-P., Corthésy-Blondin, L., Plourde-Léveillé, L., Dargis, L., & Mishara, B. L. (2018). The Darknet and suicide. *Journal of Affective Disorders*, 241, 127-132. https://doi.org/10.1016/j.jad.2018.08.028

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review*, 27(4), 237-254. https://doi.org/10.1177/1057567717709498

Mosco, V. (2004). *The Digital* Sublime. The MIT Press.

Mosco, V., & Foster, D. (2001). Cyberspace and the End of Politics. *Journal of Communication Inquiry*, 25(3), 218-236.

Müller, J.-W. (2014). On Conceptual History. In: McMahon, D. M., & Moyn, S. (2014). *Rethinking Modern European Intellectual History*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199769230.003.0004

Natale, S. (2016). There Are No Old Media. *Journal of Communication*, 66(4), 585-603. https://doi.org/10.1111/jcom.12235

Natale, S., & Balbi, G. (2014). Media and the Imaginary in History. *Media History*, 20(2), 203-218. https://doi.org/10.1080/13688804.2014.898904

Natale, S., & Ballatore, A. (2014). The web will kill them all: new media, digital utopia, and political struggle in the Italian 5-Star Movement. *Media, Culture & Society*, 36(1), 105-121. https://doi.org/10.1177/0163443713511902

Near, J. P., & Miceli, M. P. (1996). Whistle-Blowing: Myth and Reality. *Journal of Management*, 22(3), 507-526. https://doi.org/10.1177/014920639602200306

Negri, S. (2016). The Medicrime Convention: Combating Pharmaceutical Crimes through European Criminal Law and beyond. *New Journal of European Criminal Law*, 7(3), 350-367. https://doi.org/10.1177/203228441600700308

Negroponte, N. (1995). *Being Digital*. Hodder & Stoughton.

Neuendorf, K. A. (2002). *The Content Analysis Guidebook*. SAGE Publications.

Newsworks. (11th December 2019). The Guardian. Retrieved 27th December 2019, from Newsworks website: https://www.newsworks.org.uk/the-guardian

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

Norman, D. (2002). *The design of everyday things*. Basic Books.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., & Shakarian P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, 7-12. https://doi.org/10.1109/ISI.2016.7745435

O'Reilly, T. (2007). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *International Journal of Digital Economics*, 65, 17-37. https://mpra.ub.uni-muenchen.de/4580/

O'Rourke, C., & Kerr, A. (2017). Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers. *Westminster Papers in Communication and Culture*, 12(3), 21-36. http://doi.org/10.16997/wpcc.264

Ofcom. (24th July 2019). News Consumption in the UK: 2019. Retrieved 10th December 2019, from Ofcom website: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/157914/uk-news-consumption-2019-report.pdf

Office for National Statistics. (20th May 2016). *Internet users in the UK: 2016*. Retrieved 30th April 2017, from ONS website: http://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016

Oliveira, E., Natarajan, M., & da Silva, B. (2019). Bus Robberies in Belo Horizonte, Brazil: Solutions for Safe Travel. *Crime & Delinquency*. https://doi.org/10.1177/0011128719871547

Olston, C., & Najork, M. (2010). Web Crawling. *Foundations and Trends in Information Retrieval*, 4(3), 175-246. https://doi.org/10.1561/1500000017

Omand, D. (2015). The Dark Net: Policing the Internet's Underworld. *World Policy Journal*, 32(4), 75-82. https://doi.org/10.1177/0740277515623750

Orgad, S. (2012). *Media Representation and the Global Imagination*. Polity Press.

Osborn, M. (1967). Archetypal metaphor in rhetoric: The light-dark family. *Quarterly Journal of Speech*, 53(2), 115-126. https://doi.org/10.1080/00335636709382823

Owenson, G., Cortes, S., & Lewman, A. (2018). The darknet's smaller than we thought: the life cycle of Tor Hidden Services. *Digital Investigation*, 27, 17-22. https://doi.org/10.1016/j.diin.2018.09.005

Oz, M., Zheng, P., & Chen, G. M. (2018). Twitter versus Facebook: Comparing incivility, impoliteness, and deliberative attributes. *New Media & Society*, 20(9), 3400-3419. https://doi.org/10.1177/1461444817749516

Paltridge, B. (2006). *Discourse Analysis: An Introduction*. Continuum.

PAMCo. (September 2019). *PAMCo Newsbites*. Retrieved 10th December 2019, from PAMCo website: https://pamco.co.uk/news/newsletter-q3-2019/index.html

Papacharissi, Z. (2002). The Presentation of Self in Virtual Life: Characteristics of Personal Home Pages. *J&MC Quarterly*, 79(2), 643-660.

Papathanassopoulos, S. (2015). Privacy 2.0. *Social Media + Society*. https://doi.org/10.1177/2056305115578141

Pardhasaradhi, Y., & Rao, V. N. (2014. Women Empowerment: Information Technology as a Critical Input. *Indian Journal of Public Administration*, 60(3), 515-526.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, 40(2), 215-236. https://doi.org/10.1177/0093650211418338

Paulus, T. M., Lester, J. N., & Britt, V. G. (2013). Constructing Hopes and Fears Around Technology: A Discourse Analysis of Introductory Qualitative Research Texts. *Qualitative Inquiry*, 19(9), 639-651. https://doi.org/10.1177/1077800413500929

Pedley, P. (2002). Why you can't afford to ignore the invisible Web. *Business Information Review*, 19(1), 23-31. http://doi.org/10.1177/0266382024238257

Pesch, U., & Ishmaev, G. (2019). Fictions and frictions: Promises, transaction costs and the innovation of network technologies. *Social Studies of Science*, 49(2), 264-277. https://doi.org/10.1177/0306312719838339

Phelan, J. (2014). Voice, tone, and the rhetoric of narrative communication. *Language and Literature*, 23(1), 49-60. https://doi.org/10.1177/0963947013511723

Piranneiad, A., & Janssen, M. (2019). Internet and political empowerment: Towards a taxonomy for online political empowerment. *Information Development*, 35(1), 80-95. https://doi.org/10.1177/0266666917730118

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293-310. https://doi.org/10.1177/1461444816661553

Poincaré, H. (1906). The Milky Way and the Theory of Gases. *Popular Astronomy*, 14, 475-488.

Postman, N. (1997). Defending ourselves against technology. *Bull. Sci. Tech. Soc.*, 17(5-6), 229-233). http://adsabs.harvard.edu/full/1906PA.....14..475P

Postman, N. (2004). The Information Age: A Blessing or a Curse? *Harvard International Journal of Press/Politics*, 9(2), 3-10. https://doi.org/10.1177/1081180X04263457

Qin, J., Zhou, Y., Lai, G., Reid, E., Sageman, M., & Chen, H. (2005). The Dark Web Portal Project: Collecting and Analyzing the Presence of Terrorist Groups on the Web. In: Kantor P. et al. (eds) Intelligence and Security Informatics. ISI 2005. *Lecture Notes in Computer Science*, vol 3495. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11427995_78

Rama Murthy, S., & Mani, M. (2013). Discerning Rejection of Technology. *SAGE Open*. https://doi.org/10.1177/2158244013485248

Reah, D. (2002). *The language of newspapers*. Routledge.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Protocols using anonymous connections: Mobile applications. *Security Protocols: 5th International Workshop*, 13-23.

Riffe, D., Lacy, S., & Fico, F.G. (2005). *Analyzing Media Messages. Using Quantitative Content Analysis in Research*. Lawrence Erlbaum Associates' Publishers.

Robards, B., & Lincoln, S. (2016). Making It "Facebook Official": Reflecting on Romantic Relationships Through Sustained Facebook Use. *Social Media + Society*. https://doi.org/10.1177/2056305116672890

Roessler, B., & Mokrosinska, D. (2013). Privacy and social interaction. *Philosophy & Social Criticism*, 39(8), 771-791. https://doi.org/10.1177/0191453713494968

Ross, J. E. (2007). The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany. *American Journal of Comparative Law*, 55, 493-579.

Rothberg, R. L., & Stith, K. (2018). Fentanyl: A Whole New World? *The Journal of Law, Medicine & Ethics*, 46(2), 314-324. https://doi.org/10.1177/1073110518782937

Salmon, P. M., Lane, B. R., Desmond, D., Cherney, A., Kulatilleke, G., Matthews, A., Lacey, D., & Stanton, N. A. (2019). Breaking bad systems with Human Factors and Ergonomics: Using Work Domain Analysis to identify strategies to disrupt trading in dark net marketplaces. *Proceedings of the Human Factors and Ergonomics Society Annual Meeti*ng, 63(1), 458-462. https://doi.org/10.1177/1071181319631315

Sandvig, C. (2013). The Internet as Infrastructure. In: Dutton, W. H. (2013). *The Oxford Handbook of Internet Studies*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199589074.013.0005

Santos, M., & Faure, A. (2018). Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. *Social Media + Society*. https://doi.org/10.1177/2056305118795876

Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019). Understanding online anonymity. *Media, Culture & Society*, 41(4), 557-564. https://doi.org/10.1177/0163443719842074

Schaefer, T., & Fordan, R. (2014). Balance and Bias in Network Evening News Coverage of Presidential State of the Union Addresses. *Electronic News*, 8(4), 274-289. https://doi.org/10.1177/1931243114567570

Schlosser, E. (2002). *Fast Food Nation: What the All-American Meal is Doing to the World*. Penguin.

Schmidt, H. C. (2015). Student Newspapers Show Opinion Article Political Bias. *Newspaper Research Journal*, 36(1), 6-23. https://doi.org/10.1177/0739532915577959

Schraube, E. (2009). Technology as Materialized Action and Its Ambivalences. *Theory & Psychology*, 19(2), 296-312. https://doi.org/10.1177/0959354309103543

Scolari, C. A. (2009). Mapping conversations about new media: the theoretical field of digital communication. *New Media & Society*, 11(6), 943-964. https://doi.org/10.1177/1461444809336513

Seddon, T. (2019). Markets, Regulation and Drug Law Reform: Towards a Constitutive Approach. *Social & Legal Studies*. https://doi.org/10.1177/0964663919868756

Sharon, T., & John, N. A. (2018). Unpacking (the) secret: Anonymous social media and the impossibility of networked anonymity. *New Media & Society*, 20(11), 4177-4194. https://doi.org/10.1177/1461444818768547

Shestakov, D. (2008). Search Interfaces on the Web: Querying and Characterizing. *TUCS Dissertations*, 104. https://www.utupub.fi/bitstream/handle/10024/38506/diss2008shestakov.pdf?sequence=3&isAllowed=y

Shorey, S., & Howard, P. N. (2016). Automation, Big Data, and Politics: A Research Review. *International Journal of Communications*, 10(2016), 5032-5055.

Silverstone, R. (1999). *Why Study the Media?* SAGE Publications.

Simonson, P. (2014). Reinventing Invention, Again. *Rhetoric Society Quarterly*, 44(4), 299-322. Https://doi.org/10.1080/02773945.2014.938862

Singh, M. P. (2002). Deep Web Structure. *IEEE Internet Computing*, 4-5.

Skovsgaard, M. (2014). A tabloid mind? Professional values and organizational pressures as explanations of tabloid journalism. *Media, Culture & Society*, 36(2), 200-218. https://doi.org/10.1177/0163443713515740

Smirnova, O., & Holt, T. J. (2017). Examining the Geographic Distribution of Victim Nations in Stolen Data Markets. *American Behavioral Scientist*, 61(11), 1403-1426. https://doi.org/10.1177/0002764217734270

Smith, G. J. (2018). Data doxa: The affective consequences of data practices. *Big Data & Society*. https://doi.org/10.1177/2053951717751551

Smith, T. A. (2017). The Free Speech Vernacular: Conceptual Confusions in the Way We Speak About Speech. *Texas Review of Law & Politics*, 22(1), 57-92. https://ssrn.com/abstract=3166234

Soroka, S., Daku, M., Hiaeshutter-Rice, D., Guggenheim, L., & Pasek, J. (2018). Negativity and Positivity Biases in Economic News Coverage: Traditional Versus Social Media. *Communication Research*, 45(7), 1078-1098. https://doi.org/10.1177/0093650217725870

Sotirakopoulos, N. (2018). Cryptomarkets as a libertarian counter-conduct of resistance. *European Journal of Social Theory*, 21(2), 189-206. https://doi.org/10.1177/1368431017718534

Spohr, D. (2017). Fake news and ideological polarization: Filter bubbles and selective exposure on social media. *Business Information Review*, 34(3), 150-160. https://doi.org/10.1177/0266382117722446

Spolsky, B. (1998). *Sociolinguistics*. Oxford University Press.

Sternheimer, K. (2007). Do Video Games Kill? *Contexts*, 6(1), 13-17. https://doi.org/10.1525/ctx.2007.6.1.13

Stiegler, B. (1998). *Technics and Time, 1: The Fault of Epimetheus*. Stanford University Press.

Streeter, T. (2011). *The net effect: romanticism, capitalism, and the Internet*. New York University Press.

Striphas, T. (2015). Algorithmic culture. *European Journal of Cultural Studies*, 18(4-5), 395-412. https://doi.org/10.1177/1367549415577392

Sturken, M., Thomas, D., & Ball-Rokeach, S. (2004). *Technological Visions: The Hopes and Fears That Shape New Technologies*. Temple University Press.

Su, M. C. (2008). Inside the Web: A Look at Digital Libraries and the Invisible/Deep Web. *Journal of Educational Technology Systems*, 37(1), 71-82. https://doi.org/10.2190/ET.37.1.f

Sui, D., Caverlle, J., & Rudesill, D. (2015). *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*. Wilson Center.

Surette, R. (1992). Methodological Problems In Determining Media Effects On Criminal Justice: A Review And Suggestions For The Future. *Criminal Justice Policy Review*, 6(4), 291-310.

Swanlund, D., & Schuurman, N. (2019). Resisting geosurveillance: A survey of tactics and strategies for spatial privacy. *Progress in Human Geography*, 43(4), 596-610. https://doi.org/10.1177/0309132518772661

Taylor, C. (2004). *Modern Social Imaginaries*. Duke University Press.

Taylor, S. (2008). Outside the outsiders: Media representations of drug use. *Probation Journal*, 55(4), 369-387. https://doi.org/10.1177/0264550508096493

Theng, Y.-L., Lee, E. A., Chu, S. K.-W., Lee, C. W. Y., Chiu, M. M.-L., & Chan, R. C. H. (2016). Scaffolding in information search: Effects on less experienced searchers. *Journal of Librarianship and Information Science*, 48(2), 177-190. https://doi.org/10.1177/0961000615595455

Thompson, L. (2018). "I can be your Tinder nightmare": Harassment and misogyny in the online sexual marketplace. *Feminism & Psychology*, 28(1), 69-89. https://doi.org/10.1177/0959353517720226

Thurlow, C. (2006), From Statistical Panic to Moral Panic: The Metadiscursive Construction and Popular Exaggeration of New Media Language in the Print Media. *Journal of Computer-Mediated Communication*, 11(3), 667-701. https://doi.org/10.1111/j.1083-6101.2006.00031.x

Troullinou, P. (2017). Rethinking Privacy and Freedom of Expression in the Digital Era: An Interview with Mark Andrejevic. *Westminster Papers in Communication and Culture*, 12(3), 72-77. https://doi.org/10.16997/wpcc.270

Turkle, S. (1995). *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster Paperbacks.

Turkle, S. (2005). *The Second Self: Computers and the Human Spirit*. The MIT Press.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy*, 56(2018), 176-186. https://doi.org/10.1016/j.drugpo.2018.01.022

van Baalen, S. (2018). 'Google wants to know your location': The ethical challenges of fieldwork in the digital age. *Research Ethics*, 14(4), 1-17. https://doi.org/10.1177/1747016117750312

Van Deursen, A. J., & Helsper, E. J. (2018). Collateral benefits of Internet use: Explaining the diverse outcomes of engaging with the Internet. *New Media & Society*, 20(7), 2333-2351. https://doi.org/10.1177/1461444817715282

Van Dijck, J. (2013). *The Culture of Connectivity: a Critical History of Social Media*. Oxford University Press.

van Dijk, T. A. (1995). Discourse Semantics and Ideology. *Discourse & Society*, 6(2), 243-289. https://doi.org/10.1177/0957926595006002006

van Dijk, T. A. (2013). Principles of critical discourse analysis. *Discourse & Society*, 4(2), 249-283.

van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*, 61(11), 1244-1266. https://doi.org/10.1177/0002764217734271

Van Hout, M. C., & Bingham, T. (2013). 'Silk Road,' the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, 24(5), 385-391. https://doi.org/10.1016/j.drugpo.2013.01.005

Vargo, C. J., Guo, L., & Amazeen, M. A. (2018). The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. *New Media & Society*, 20(5), 2028-2049. https://doi.org/10.1177/1461444817712086

Vasterman, P. L. M. (2005). Media-Hype: Self-Reinforcing News Waves, Journalistic Standards and the Construction of Social Problems. *European Journal of Communication*, 20(4), 508-530. https://doi.org/10.1177/0267323105058254

Venger, O. (2019). The use of experts in journalistic accounts of media events: A comparative study of the 2005 London Bombings in British, American, and Russian newspapers. *Journalism*, 20(10), 1343-1359. https://doi.org/10.1177/1464884919830479

Voorhees, E. M. (1999). Natural Language Processing and Information Retrieval. In Pazienza, M. T., *Information Extraction: Towards Scalable, Adaptable Systems* (pp. 32-48). Springer-Verlag.

Wark, M. (2006). Hackers. *Theory, Culture & Society*, 23(2-3), 320-322.

Weimann, G. (2016a). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, 39(3), 195-206, https://doi.org/10.1080/1057610X.2015.1119546

Weimann, G. (2016b). Terrorist Migration to the Dark Web. *Perspectives on Terrorism*, 10(3), 40-44. https://www.jstor.org/stable/26297596

Weinberg, L. (2017). Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden. *Westminster Papers in Communication and Culture*, 12(3), 5-20. https://doi.org/10.16997/wpcc.258

Welch, M., Fenwick, M., & Roberts, M. (1997). Primary Definitions of Crime and Moral Panic: A Content Analysis of Experts' Quotes in Feature Newspaper Articles on Crime. *Journal of Research in Crime and Delinquency*, 34(4), 474-494. https://doi.org/10.1177/0022427897034004004

Westin, A. F. (1967). *Privacy and Freedom*. Athenum.

WhatsApp. (24th April 2018). WhatsApp Privacy Policy. Retrieved on 10th December 2019, from WhatsApp website: https://www.whatsapp.com/legal/?eea=1#privacy-policy

Williams, A. E. (2013). Metaphor, Media, and the Market. *International Journal of Communication*, 7, 1404-1417.

Williams, R. (1975). *Television: Technology and Cultural Form*. Schocken Books.

Winkel, O. (2003). Electronic Cryptography: Chance or Threat for Modern Democracy? *Bulletin of Science, Technology & Society*, 23(3), 185-191. https://doi.org/10.1177/0270467603023003006

Wood, D. (2001). *The hidden geography of transnational surveillance : social and technological networks around signals intelligence sites* (Unpublished doctoral dissertation). Newcastle University, Newcastle, United Kingdom.

Wright, A. Searching the Deep Web. Communications of the ACM, 51(10), 14-15. http://doi.org/10.1145/1400181.1400187

Wring, D., & Deacon, D. (2010). Patterns of press partisanship in the 2010 General Election. British Politics, 5(4), 436-454. https://doi.org/10.1057/bp.2010.18

Wu, T.-Y., & Atkin, D. J. (2018). To comment or not to comment: Examining the influences of anonymity and social support on one's willingness to express in online news discussions. *New Media & Society*, 20(12), 4512-4532. https://doi.org/10.1177/1461444818776629

Wu, W., Doan, A., & Yu, C. (2006). WebIQ: Learning from the Web to Match Deep-Web Query Interfaces. In *22nd International Conference on Data Engineering (ICDE'06)*, Atlanta, GA, USA, 2006, 44-44. https://doi.org/10.1109/ICDE.2006.172

Wu, W., Yu, C., Doan, A., & Meng, W. (2004). An interactive clustering-based approach to integrating source query interfaces on the deep Web. In *Proceedings of the 2004 ACM SIGMOD international conference on Management of data (SIGMOD '04)*. ACM, New York, NY, USA, 95-106. https://doi.org/10.1145/1007568.1007582

Yamada, Y., Craswell, N., Nakatoh, T., & Hirokawa, S. (2004). Testbed for information extraction from deep web. In *Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters (WWW Alt. '04*), ACM, New York, NY, USA, 346-347. https://doi.org/10.1145/1013367.1013468

Yang, F. (2016). Rethinking China's Internet censorship: The practice of recoding and the politics of visibility. *New Media & Society*, 18(7), 1364-1381. https://doi.org/10.1177/1461444814555951

YouGov. (7th March 2017). *How left or right-wing are the UK's newspapers?* Retrieved on 10th December 2019, from YouGov website: https://yougov.co.uk/topics/politics/articles-reports/2017/03/07/how-left-or-right-wing-are-uks-newspapers

Zajácz, R. (2013). WikiLeaks and the problem of anonymity: A network control perspective. *Media, Culture & Society*, 35(4), 489-505. https://doi.org/10.1177/0163443713483793

Zhao, M. (2019). The Illicit Supply of New Psychoactive Substances Within and From China: A Descriptive Analysis. *International Journal of Offender Therapy and Comparative Criminology*. https://doi.org/10.1177/0306624X19866119

Ziccardi, G. (2013). *Resistance, Liberation Technology and Human Rights in the Digital Age*. Springer.

Appendix

British Media Representation of the Deep Web technologies: Codebook for Content Analysis

This research aims to understand how six British newspapers represent the Deep Web technologies on their news coverage. For that, the quantitative method approach of content analysis will be applied to a range of newspapers' articles mentioning these systems and results will be interpreted to understand the overall media representation.

Sampling

This work uses LexisNexis databases to collect articles from the following British newspapers: *Daily Mail*, *Daily Mirror*, *Daily Telegraph*, *The Guardian*, *The Times*, and *The Sun*. The time frame is between 1st January 1989 and 31st December 2017.

Terms of Inclusion

This codebook is suitable for articles mentioning any of the following terms: "dark internet," "dark net," "dark side of the internet," "dark side of the web," "dark web," "darknet," "darkweb," "deep internet," "deep web," "hidden internet," "hidden web," "internet dark side," "invisible internet," "invisible web," "non-indexable internet," "non-indexable web," "silk road," "silkroad," "tor browser," "tor network," "tor system," "undernet," "underweb," "underworld of the internet," "underworld of the web," "web dark side," and "web underworld."

Unitization

Each newspaper article will be analysed separately and considered as a case. Different elements of these cases are then coded according to the variables and values set out below.

CASE IDENTIFICATION VARIABLES				
ID	NAME	CODE (VALUE)	CODE LABEL	CODING INSTRUCTIONS
V01	ID Number			Newspaper number + Date (DDMMYYYY) + Number
V02	Date			DD/MM/YYYY
V03	Newspaper	1	Daily Mail	In which of these newspapers the article was published
		2	Daily Mirror	
		3	The Guardian	
		4	Daily Telegraph	
		5	The Sun	
		6	The Times	
V04	Type of article	1	News article	Specify the kind of article on the newspaper
		2	Editorial	
		3	Comment, opinion or reader letter	
		4	Review (book, movie, TV show, radio series and others)	

		5	Interview	
		6	Fiction	
V05	Length of the text			Number of words

CONTENT VARIABLES				
ID	NAME	CODE (VALUE)	CODE LABEL	CODING INSTRUCTIONS
V06	Does the headline mention Deep Web or related terms (listed aside)?	1	Yes	If the headline of the article mentions any of these terms: "dark side of the internet" or "dark side of the web" or "dark internet" or "dark net" or "darknet" or "dark web" or "darkweb" or "deep internet" or "deep net" or "deep web" or "hidden internet" or "hidden web" or "internet dark side" or "invisible internet" or "invisible web" or "non-indexable web" or "non-indexable internet" or "tor browser" or "tor network" or "tor system" or "undernet" or "underweb" or

				"underworld of the internet" or "underworld of the web" or "web dark side" or "web underworld" or "silkroad" or "silk road"
		2	No	If the headline doesn't mention any of those terms
V07	Which of these terms the headline mentions? (In the case of more than one, use the first one)	1	Dark Internet	
		2	Dark Net	Also "darknet"
		3	Dark side	Referring to one of these variables: "dark side of the internet" or "dark side of internet" or "internet dark side" or "dark side of the web" or "dark side of web" or "web dark side"
		4	Dark Web	Also "darkweb"
		5	Deep Internet	
		6	Deep Web	
		7	Hidden Internet	
		8	Hidden Web	

		9	Invisible Internet	
		10	Invisible Web	
		11	Non-Indexable Web	
		12	Silk Road	Also “Silkroad” and “Silk Road 2.0”
		13	Tor	Also “The Onion Router,” “Onion Routing” and “Tor Project”
		14	Tor Browser	
		15	Tor Network	
		16	Tor System	
		17	Undernet	
		18	Underweb	
		19	Underworld	Referring to one of these variables: “underworld of the internet" or "underworld of the web" or "web underworld"
		20	Deep Net	
		99	Not Applicable	

V08	Does the headline of the article mention some of these activities? (Select the main one when more than one is mentioned	1	Black market	Headline mentions black market on Deep Web in a generic way (not specifying if it is focused on drugs, guns or stolen items, or mentioning multiple appropriations), Silk Road (and similar websites) or "trade"
		2	Cybercrime	Headline mentions any cyber or digital attack or threat, victim of leaking of personal (such as celebrity photo) or corporate information, stealing of identity, online scams, and/or computer viruses, when the word hacker or hacking is not used
		3	Drugs	Headline mentions specifically some kind of drug, poison, toxin, overdose, medicine addiction, death caused by drugs, legal highs, or drugs market available on Deep Web
		4	Espionage	Headline mentions any case in which Deep Web was used to commit espionage

				against any government
		5	Financial	Headline mentions financial issues such as cloning of credit card, Bitcoin, currencies, financial fraud, money laundering, or another crime directly related to money and banks
		6	Gambling	Headline mentions gambling addiction and crimes related to gambling
		7	Weapons	Headline mentions specifically some kind of weapons (including nuclear drones, bombs, biological, and others) or guns market available on Deep Web
		8	Hacking	Headline mentions a specific person that is charged, arrested or persecuted for running a website on Deep Web, a person considered a hacker (such as Dread Pirate Roberts), or a hacking organisation, or a person or company that is victim of hacking –

				only when the word "hacker," "hacking" or "hacktivism" is applied on the title
		9	Kidnapping	Headline mentions kidnapping of a person, or related issues, such as hostage, ransom, specifying the reason (such as selling a person for sexual slavery) or not
		10	Mass murder	Headline mentions any kind of mass murder (when not considered a terrorist attack) that was planned or done using Deep Web systems
		11	Offline Crime	Headline mentions generically crimes that are committed offline, such as murder, serial killer, rape, fake tickets or documents, environment crimes, and/or criminals (not specified in the other options)
		12	Paedophilia	Headline mentions cases of paedophilia, and/or pornography, abuse or exploitation of children

		13	Pornography	Headline mentions cases of pornography, porn addiction, BDSM (excluding cases with children)
		14	Terrorism	Headline mentions terrorist attack, terrorist organization, jihadis, plans for a terrorist attack, or fight against terror (including states or organizations considered enemies on this fight)
		15	Whistle-blowing	Headline mentions to whistle-blowers, or the leaking of NSA files, mentioning Edward Snowden, WikiLeaks and software Prism (used by the US government for surveillance)
		99	Not Applicable	Headline doesn't mention any crime
V09	Does the article refer to surveillance practices?	1	On the headline	Just the headline mentions surveillance practices (including censorship, over watching, state control, vigilance, tracking, digital footprints, face recognition, electronic footprint,

				monitoring, cookies, spies)
		2	On the text	Just the text mentions surveillance practices
		3	Both on the headline and on the text	
		4	Nor on the headline or on the text	
V10	Does the article refer to privacy issues?	1	On the headline	Just the headline mentions privacy (including private life and communications, secrecy, hiding, personal data, personal details, encrypted communication)
		2	On the text	Just the text mentions privacy issues
		3	Both on the headline and on the text	
		4	Nor on the headline or on the text	
V11	Does the article refer to anonymity?	1	On the headline	Just the headline mentions anonymity (including anonymous communications, invisibility, hiding

				identity, namelessness, unknown person, alias, codename, pseudonym)
		2	On the text	Just the text mentions anonymity issues
		3	Both on the headline and on the text	
		4	Nor on the headline or on the text	
V12	Does the article refer to authoritarianism?	1	On the headline	Just the headline mentions authoritarian states and/or regimes and/or practices (including autocracy, despotism, dictatorship, fascism, monocracy, totalitarianism, tyranny) that go against the freedom of speech
		2	On the text	Just the text mentions authoritarian practices
		3	Both on the headline and on the text	
		4	Nor on the headline or on the text	

V13	Which Deep Web related term the article uses (referring to the first occurrence of the term on the text)?	1	Dark Internet	
		2	Dark Net	Also “darknet”
		3	Dark side	Referring to one of these variables: "dark side of the internet" or "dark side of internet" or "internet dark side" or "dark side of the web" or "dark side of web" or "web dark side"
		4	Dark Web	Also “darkweb”
		5	Deep Internet	
		6	Deep Web	
		7	Hidden Internet	
		8	Hidden Web	
		9	Invisible Internet	
		10	Invisible Web	
		11	Non-Indexable Web	
		12	Silk Road	Also “Silkroad” and “Silk Road 2.0”
		13	Tor	Also “The Onion Router,” “Onion

				Routing” and “Tor Project”
		14	Tor Browser	
		15	Tor Network	
		16	Tor System	
		17	Undernet	
		18	Underweb	
		19	Underworld	Referring to one of these variables: “underworld of the internet" or "underworld of the web" or "web underworld"
		20	Deep Net	
		99	Not Applicable	
V14	Which Deep Web related term the article uses on second place (referring to the occurrence of a different term on the same text)?	1	Dark Internet	
		2	Dark Net	Also “darknet”
		3	Dark side	Referring to one of these variables: "dark side of the internet" or "dark side of internet" or "internet dark side" or "dark side of the

				web" or "dark side of web" or "web dark side"
		4	Dark Web	Also “darkweb”
		5	Deep Internet	
		6	Deep Web	
		7	Hidden Internet	
		8	Hidden Web	
		9	Invisible Internet	
		10	Invisible Web	
		11	Non-Indexable Web	
		12	Silk Road	Also “Silkroad” and “Silk Road 2.0”
		13	Tor	Also “The Onion Router,” “Onion Routing” and “Tor Project”
		14	Tor Browser	
		15	Tor Network	
		16	Tor System	
		17	Undernet	

		18	Underweb	
		19	Underworld	Referring to one of these variables: "underworld of the internet" or "underworld of the web" or "web underworld"
		20	Deep Net	
		99	Not Applicable	
V15	Does the article use some of the Deep Web related terms with quotation marks (on the headline or text)?	1	On the headline	One or more of these terms is written between quotation marks on the headline: "dark side of the internet" or "dark side of the web" or "dark internet" or "dark net" or "darknet" or "dark web" or "darkweb" or "deep internet" or "deep net" or "deep web" or "hidden internet" or "hidden web" or "internet dark side" or "invisible internet" or "invisible web" or "non-indexable web" or "non-indexable internet" or "tor browser" or "tor network" or "tor system" or "undernet"

				or "underweb" or "underworld of the internet" or "underworld of the web" or "web dark side" or "web underworld" or "silkroad" or "silk road"
		2	On the text	At least one of these terms is written between quotation marks on the text
		3	Both on the headline and on the text	
		4	Nor on the headline or on the text	
V16	Does the article use the expression "so-called" to refer to Deep Web (on the headline and/or text)?	1	On the headline	The expression "so-called" is associate with Deep Web and/or related terms on the headline
		2	On the text	The expression "so-called" is associate with Deep Web and/or related terms on the text
		3	Both on the headline and on the text	
		4	Nor on the headline or on the text	

V17	Does the article offer an apposition (explanation or definition) for the term?	1	Yes	Article explains what Deep Web systems are using apposition, definitions, concepts, comparisons, analogies, or other linguistic resource
		2	No	Article takes for granted what the system is
V18	In the case that the article offers an apposition, what is the source of the information?	1	Academic	When the source is specialist on the topic and connected to a university (which is mentioned on the article)
		2	Book	When the source is a sentence from a book, so the title and/or author is cited on the article
		3	Corporate	When the source is specialist on some topic and related to a company (which is mentioned on the article), or a corporative spokesperson
		4	Government	When the source is member of political parties, government department, NATO (excluding law enforcement and police)

		5	Hacker	When the source is connected to a hacker organization (such as Anonymous or Global Vigilance) or assumes itself as a member of the hacker community (which is mentioned on the article)
		6	Law professional	When the source is member of the justice system (such as judge, lawyer, persecutor), excluding police
		7	Civil society organization	When the source is connected with organizations that advocate for privacy rights and/or against surveillance (which is mentioned on the article), civil organizations, charity, activists
		8	Police	When the source is member of police, military or intelligence agencies (such as Scotland Yard and FBI)
		9	Specialist	When the person is consulted because of professional knowledge, such as IT consultants, cyber security experts, researchers,

				psychiatrists, journalists, and others, when the company or institution is not mentioned on the article
		10	News	When the source is a previous news article or report for TV, internet or radio, made by the press
		98	Not Specified	Article gives a generic definition without specified the source of the information
		99	Not Applicable	When there is no definition
V19	Which attribute is associated with or used to describe Deep Web or related terms (considering the first one to be mentioned on the same sentence as Deep Web or related terms)?	1	Anonymous	Also "anonymising"
		2	Black-market	
		3	Criminal	Also "crime facilitator"
		4	Encrypted	Also "highly encrypted" or "heavily encrypted"
		5	Hidden	Also "used to hide" or "a way of hiding"
		6	Illegal	
		7	Illicit	

		8	Inaccessible	Also “not accessible”
		9	Invisible	
		10	Lawless	Also “beyond the law” and “unlawful”
		11	Not viewable	
		12	Resilient	
		13	Secretive	Also “secret”
		14	Secure	
		15	Shadowy	Also “shady” or “shadier”
		16	Unlisted	Also “not listed”
		17	Unpoliced	
		18	Unregulated	
		19	Unreachable	Also “beyond the reach”
		20	Untraceable	Also “that cannot be traced” or “without being traced”
		21	Parallel	
		22	Notorious	

		23	Murky	
		24	Noxious	
		25	Refuge	
		26	Harder	Also “hard-to-access” or “hard-to-track”
		27	Restricted	
		28	Booming	
		29	Undetectable	
		30	Treasure	
		31	Uncharted	
		32	Huge	
		33	Safe	Also “safer”
		34	Underground	
		35	Wonderland	
		36	Infamous	
		37	Sinister	
		38	Popular	

		39	Complex	
		40	Free	
		41	Dark	Also “darkest”
		42	Solution	
		43	Shield	
		44	Comprehensive	
		45	Interesting	
		46	Buried	
		47	Route	
		48	Sophisticated	
		49	Vast	
		50	Specialised	Also “special” and “specialist”
		51	Nasty	Also “nastier”
		52	Drug-dealing	
		53	Dodgy	
		54	New phenomenon	

		55	Sick	
		56	Ugly	
		57	Under the radar	Also “beneath the radar”
		58	Chilling	
		59	Difficult	
		60	Covert	
		61	Grim	
		62	Abnormal	Also “not normal”
		63	Grey	
		64	Bazaar	
		65	Large	
		66	Underside	
		67	Major	
		68	Mysterious	
		69	Chaotic	
		70	Not indexed	

		71	Private	
		72	Vile	
		99	Not applicable	
V20	Which term is associated with people that use Deep Web systems on the article (considering the first one to be mentioned on the same paragraph)?	1	Buyer	
		2	Consumer	
		3	Coward	
		4	Criminal	Also "organised crime," "people engaging in criminal activities," "crime group" and "cybercriminal"
		5	Faceless	Also "faceless person"
		6	Hacker	Also "hacking group"
		7	Outlaw	
		8	Paedophile	Also "paedos"
		9	Pervert	
		10	Seller	
		11	Terrorist	Also "terror leader," "terror network" and "terrorist group"

		12	Troll	
		13	Pornographer	
		14	Abuser	
		15	User	
		16	Dealer	Also “drug dealer” and “arms dealer”
		17	Crook	
		18	Suspect	Also “suspected of …”
		19	Player	
		20	Fraudster	
		21	Researcher	Also “person conducting a research”
		22	Whistle-blower	
		23	Drug user	
		24	Predator	
		25	Community	
		26	Connoisseur	

		27	Activist	
		28	Extremist	
		29	Jihadist	Also “jihadis”
		30	Offender	Also “sex offender”
		31	Addict	
		32	Gang	Also “gangland,” “crime gang” and “gangster”
		33	Journalist	
		34	Government	
		35	State	
		36	Trafficker	
		37	Recruiter	
		38	Conspirator	
		39	Kidnapper	
		40	Peddler	
		41	Defendant	

		42	Ruler	
		43	Student	
		44	Costumer	
		45	Supplier	Also “drug supplier” or “arm supplier”
		46	Thief	
		47	Killer	
		48	Youngster	Also “young people”
		49	Smuggler	
		50	Syndicate	
		51	Trader	
		52	Fiend	
		53	Fanatic	
		54	Geek	Also “computer geek”
		55	Member	
		56	Backer	
		57	Troubled	Also “troubled person”

		58	Rapist	
		59	Nut	
		60	Teenager	
		61	Arab	
		62	Group	
		63	Scientist	Also “computer scientist”
		64	Bomber	Also “suicide bomber”
		65	Client	
		66	Isis member	Also “Isis activist” and “Isis sympathiser”
		67	Gunman	
		68	Visitor	
		69	Sucker	
		70	Islamist	
		71	Exploiter	
		72	Villain	Also “cyber-villain”

		73	Al-Qaeda	
		74	Molester	
		75	Captor	
		76	Cryptographer	
		77	Reject	
		78	Operator	
		79	Mafia	
		99	Not applicable	
V21	Source 1 (Code only those who are either directly quoted or paraphrased) (Use the same criteria for Source 2 to Source 12)	1	Academic	When the source is specialist on the topic and connected to a university (which is mentioned on the article)
		2	Corporate	When the source is specialist on some topic and related to a company (which is mentioned on the article), or a corporative spokesperson
		3	Government	When the source is member of political parties, government department, NATO (excluding law

				enforcement and police)
		4	Hacker	When the source is connected to a hacker organization (such as Anonymous or Global Vigilance) or assumes itself as a member of the hacker community (which is mentioned on the article)
		5	Law professional	When the source is member of the justice system (such as judge, lawyer, prosecutor, justice minister), excluding police
		6	Civil society organization	When the source is connected with organizations that advocate for privacy rights and/or against surveillance (which is mentioned on the article), civil organizations, charity, activists
		7	Police	When the source is a member of police, military or intelligence agencies (such as Scotland Yard, NCA and FBI)
		8	Specialist	When the person is consulted because of professional

				knowledge, such as IT consultants, cyber security experts, researchers, psychiatrists, journalists, "a source," and others, when the company or institution is not mentioned on the article
		9	Suspect or criminal	When the source is the person that committed the crime, or is being accused of a crime, or was planning a crime, or someone talking on their behalf (including family)
		10	Victim	When the source is a person that was impaired by some crime that is connected with Deep Web systems functionalities, or if someone is speaking in the name of this person (such as a spokesperson, family member or PR agency), or if the person is a witness of a crime
		11	Case	When the source is a neutral person used to exemplify something on the

				article but is not an expert on any topic
		99	Not applicable	
v22	Does the Source 1 offer an opinion about Deep Web or related systems? (Use the same criteria for Source 2 to Source 12)	1	Yes	The source gives an opinion about what he/she thinks or understands of the Deep Web or related systems
		2	No	The source doesn't give an opinion or talk specifically about Deep Web or related systems
		99	Not applicable	