Freedom in cyberspace: Exploring what it means to be negatively and positively free in cyberspace

Jorna, Melle

Freedom in Cyberspace

Exploring what it means to be negatively and positively free in cyberspace

By: Melle Jorna

S2520087

Word count: 7915

Justice & equality in a globalised world

Supervisor: MSc/MPhil Daemen

Leiden University

Table of contents

Introduction

Cyberspace is a domain that is of significant relevance for contemporary society, and even more so for the future. However, as an academic subject, it is relatively unexplored considering its presence in society. The largest portion of literature is dedicated to either the security aspect of cyberspace, better known as cybersecurity, or to the more technical side of cyberspace, the infrastructure making it possible. Philosophical questions that are continuously asked about conventional society, have thus far not been translated in this ever-increasingly important domain. Questions about how society ought to be designed are brought up answered throughout the ages, from ancient times all the way to the 21st century. These questions range from the origins of justice and equality to the role of institutions or the political organisation of society (Lane, 2018). These questions fall under the branch of political philosophy, which can be defined as the "philosophical reflection on how best to arrange our collective life - our political institutions and our social practices, such as our economic system and our pattern of family life" (Miller, 1998).

Most, if not all, aspects of life, from social connections, political engagement, consumption of news and even education, involve cyberspace to a certain degree. The observation that can be made is that much of contemporary life moves into the domain of cyberspace, and therefore an exploration of the application of conventional ideas of political philosophy in cyberspace is warranted. As a consequence, this research aims to explore one of the most prominent concepts in political philosophy, namely the concept of freedom, and explore the meaning of freedom in cyberspace. This paper is centred around the following research question: *What does it mean to be free in cyberspace?*

Freedom is "an elusive as well as a potent ideal" (Miller, 2017, p.1). The potency lies in the ability of the concept to provide a sense of an ideal that people ought to strive for. Despite the plethora of different ideas on freedom, freedom is considered to be essential. The elusivity of freedom is to be found in the lack of any consensus on what freedom is, which leads to freedom being subject to interpretation to a degree that it can seem incomprehensible (Berlin, 2017, p.33). Nevertheless, theories of freedom can largely be divided in two main strands, *negative* and *positive* conceptions of freedom. A negative account of freedom concerns the absence of certain constraints, this a freedom *from* something (Carter, 2022).

Predominantly, negative accounts of freedom are considering the *external* effects on one's choices, for example being coerced into making certain choices that otherwise the individual would have refrained from. On the other hand, positive freedom concerns, primarily,

the *internal* factors that affect one's choices, for example self-mastery. Also the *presence* of one's possibility to achieve something, or the access to something, is addressed in a positive account of freedom. For instance, access to drinking water or the possibility to educate oneself (Carter, 2022). In sum, negatively speaking, an individual achieves freedom through the *absence* of obstacles and restraints. Positively speaking, an individual achieves freedom through the *presence* of certain crucial possibilities and self-mastery.

To explore freedom in cyberspace, the two perspectives, negative and positive, will be combined and subsequently applied to cyberspace to form a comprehensive conception of what it means to be free in cyberspace. The combination of two accounts is justified by the nature of the concept of freedom. Since freedom is thoroughly subject to one's interpretations, it becomes difficult to obtain common ground when exploring freedom, however, by combining two contrasting ways of examining freedom, a certain degree of universality can be achieved. For the negative account of freedom, the theory of *freedom as non-domination* by Philip Pettit (1996; 1999; 1997) will be used. The non-domination account of freedom is a broad theory that encompasses the core of negative freedom, namely freedom *from* something, but extends further than the account of *freedom as non-interference* by Isaiah Berlin (1969). The non-interference account of freedom limits itself to *actual* interference, whereas, freedom as non-domination also includes the *capability* to interfere. This is crucial, because in cyberspace the *threat* of an attack is actively limiting one's functionality online. For the positive account, I will use the work by Marta Nussbaum (2000). One of the advantages to specifically Nussbaum's account is that her theory offers a more concrete perspective on the actual capabilities itself. Furthermore the capabilities approach examines *real* lives, rather than a mere conceptual deliberation (Nussbaum, 2000, pp 71-72). Besides, Nussbaum's account includes a list of concrete capabilities. The combination of the contrasting accounts of freedom will offer a broad and comprehensive understanding of freedom, to subsequently apply to cyberspace.

In the first chapter, I start off with a discussion of the theories of freedom utilised in this paper, namely the theory of *freedom as non-domination* by Philip Pettit (1999) and the *capabilities approach* by Martha Nussbaum (2000). Subsequently, in the second chapter, cyberspace is conceptualised, and the aforementioned theories of freedom are used to construct the concept of cyber freedom. The chapter is guided through two questions, namely the question of what cyberspace is, what freedom in cyberspace is. Building on the second chapter, I explore three main questions in the third chapter, namely (1) what does it mean to be free in cyberspace? (2) What is the role of cybersecurity in ensuring freedom in cyberspace? (3) How

should the state ensure freedom in cyberspace for its people? Finally, a conclusion is provided in which I briefly discuss the implications, limitations and provide a short summary.

Chapter I

In order to explore freedom in cyberspace, I first conceptualise the idea of freedom. Therefore, the subquestion of the first chapter is *what is freedom?* This conception ought to be broad, and as universal as possible so that it subsequently can be applied to cyberspace.

Freedom as non-domination

According to Pettit, freedom as non-domination is "... the sense that concerns us, then, is the position that someone enjoys when they live in the presence of other people and when, by virtue of social design, none of those others dominates them (Pettit, 1997, p. 67). In order to gain a thorough understanding, I will deconstruct the above-mentioned definition of freedom as non-domination. The notion of "The position that someone enjoys" means that freedom as non-domination concerns a certain status, a state in which domination is absent. Secondly, Pettit specifically emphasises the *presence of other people*, which means that this "status" should be achievable in a societal setting, therefore, achieving a state of non-domination through isolation from society does not make one "free". Non-domination has to be achieved through the absence of domination, not the absence of other people (Pettit, 1999, p. 66).

Then, what is *domination*? Domination, can according to Pettit (1999), best be understood if an individual has a certain power over the other, and that this power is specified by being of interfering nature as well as arbitrary. Furthermore, this power is relational, it is between individuals, or between a system and an individual. One of the essential distinctions between freedom as non-interference, as argued by Berlin (1969), and freedom of non-domination, is that this power is based on the capability to exert this power, not merely the interference itself (Pettit, 1999, p. 55). In other words, if an individual holds the power to interfere with another's choices in life, even if the individual does not actually exercise this power, then this relationship is to be characterised as a dominating relationship (Pettit, 1999, p. 51).

The question of what actually constitutes interference is a crucial one. There are three main conditions for interference. Firstly, it involves some kind of coercion of either the body, the will, or the mind (through manipulation). Secondly, the interference results per definition in a worsening of the individual's situation. Whether that was the objective of the interference, is not relevant. Thirdly, and perhaps most importantly, is the condition of the arbitrary nature of the interference. To elaborate, Pettit (1999) argues the following: "... if it is subject just to

the arbitrium, the decision or judgement, of the agent; the agent was in a position to choose it or not choose it, at their pleasure" (p. 55). Thus, the interference is not limited by direct consequences; the power is unchecked. Unchecked in the way that the power is enabled through the lack, or the flawed, presence of just controls that could limit or prevent the power from having its dominating character. As a consequence, the decision to interfere is made without any consideration of the consequences it carries for affected individuals (Pettit, 1997, p. 45). This consideration has two implications for freedom as non-domination: first, the mere fact that another individual holds the power to arbitrarily interfere in an individual's life is considered domination; and second, in order to affirm the domination, the individual must actually be able to exercise this power, if the individual is only virtually able, but not actually able, then the threat of interference is not to be considered relevant for identifying accounts of domination.

However, not all interference is included. First of all, interference that happens by accident is not to be considered a form of interference relevant for domination. The argument behind this is that the objective of Pettit's theory is to identify the individuals that are subject to the will of others, and subsequently aim to limit this form of interference. The objective is not to secure individuals against "chance" (Pettit, 1999, pp. 53-54). Secondly, context is essential, as the objective is to find instances in which the interference or threat of interference results in a worsening situation for the individual in question. Therefore, in certain occasions, an omission of something can even be considered a form of domination. If a trusted professional omits important information, which in turn adversely affects the individual's choices and possibilities, then this is also considered a dominating relationship. However, as mentioned earlier, if this omission happens through an accident, miscalculation of other forms of chance, this is to be considered outside of the scope of domination (p. 54). In sum, the status of non-domination means that an individual is, without isolating oneself, not subject to arbitrary interference by others in the individual's choices (p. 67).

But how could this situation be achieved? Pettit's answer to that essential question is explained through antipower (Pettit, 1996). Antipower is, in essence, the balancing of the power between the potentially dominated, and the individual with the dominating power. The aim is to equalise the power so that the dominator does not have the capability to interfere arbitrarily, as by balancing the power, the individual will be able to offer resistance and potentially defend itself (Pettit, 1999, p. 67). Pettit argues that if an individual has the capability to protect oneself from arbitrary interference, then domination does not occur anymore. However, Pettit also realises that this ideal defensive form might not be so plausible in reality.

Another possibility is to provide a sanctioning mechanism, thus to deter the interference by for example imprisonment. The problem with this, according to Pettit is, that this in itself is a form of interference. A constitutional approach is preferred. The constitutional authority, argues Pettit, is an agent, elected, that is introduced to the situation and subject to democratic and constitutional justification. This authority will be able to balance power by offering sanctions on interference, by doing so, the dominating power is eliminated. However, it is important that the authority itself is not dominating others (pp. 67-68).

How then can the authority legitimise its power, that could be experienced as dominating power when looking at the aforementioned conditions? Pettit (1999) argues that the authority is serving a common good, and that its interests and power should be able to be explained through their ideas, which are to be derived from the common good it aims to serve (p. 68). However, cyberspace is unique in the lack of central authorities, and therefore Pettit's ideas on how to minimise domination do not seamlessly translate into cyberspace, this is further discussed in chapter three.

The capability approach

The essence of the capabilities approach lies in the objective of determining freedom through "human functionings", which is something that an individual can *do* or *be* (Robeyns, 2016). The capabilities an individual enjoys are the vehicle to arrive at a state in which the individual can enjoy human functionings, which indicates a "worthy life". Examples of these functionings are to interact socially with others, be able to nourish, and be able to educate oneself. The subsequent question is to test whether these capabilities, which ought to be central to "humanity" are in the possession of the individual, and distinguish humans from animals (Nussbaum, 2000, pp. 71-72).

Nussbaum's theory is based around a set of defined "central capabilities", which involve the following capabilities: (1) being able to not die prematurely, nor have a "worthless" life; (2) being able to maintain good health and circumstances that promote a healthy life; (3) being able to move freely, and not be physically interfered with; (4) being able to think independently, being able to enjoy a basic education, and being able to express oneself culturally and politically; (5) being able to have emotions with other individuals, not being subject to trauma or abuse; (6) being able to be critical and "form a conception of the good"; (7) being able to engage with others, and to have the capability for justice and friendship; (8) being able to live with concern in nature, among other species; (9) being able to pursue and

enjoy recreational activities; (10) being able to participate politically, and to have one's free speech guaranteed, also being able to hold property and seek engagement on an equal footing as others (pp. 77-80).

Other theories often revolve around resources, and the distribution of these resources, for Nussbaum however, it is only important how these resources are allocated to support the individuals in being able to achieve these capabilities (p. 71). Crucially, the functionings, enables humans to live an active life, different from a life as a "herd" animal. The distinguished "human powers" of social interaction, and reasoning are central in achieving a certain state of "dignity", which according to Nussbaum, is essential for arriving at a stage in which an individual is actually "human" (p. 72).

The functionings can be seen as a certain kind of "threshold" for a human life, despite this, Nussbaum instead argues that she seeks to apply a higher threshold, one that would indicate a "truly human" life (p. 73). The capabilities that an individual enjoys, and thus provide a truly human life, also has the implication that individuals become a "bearer of value" (p.73). Another implication of individuals as bearers of value is that society ought to respect all individuals present in the polity as equal, since every individual carries the human value (p.74). However, this is not to be confused with approaching freedom as a matter for societies, groups or systems, Nussbaum emphasises that the capability approach has as unit of analysis the individual rather than any larger body. Nonetheless, organisational bodies do play a crucial role in pursuing the promotion of capabilities and thus aiming to shape a society in which *each* individual is to be considered free due to the availability for each individual to have the capabilities that make an individual truly human (p. 74).

Chapter II

Conceptualisation of cyberspace

Literature is remarkably sparse when it comes to the non-technical research into the specifics of cyberspace. Therefore, the absence of a wide plethora of contrasting definitions allows this research to utilise a single definition. The National Institute of Standards and Technology, in short, NIST, is often considered one of the, if not the, most trusted sources when it comes to cybersecurity. The NIST defines cyberspace as follows: *"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."* (NIST, 2003). When examining this definition two main elements can be identified: (1) the global domain within the information environment; (2) the interdependent network of the internet, telecommunications networks, computer systems, and embedded processors and controllers. Furthermore, the first element clearly relies on the second. Therefore, the first element can be identified as the digital environment, in which interactions, payments, information-sharing, entertainment, and all other aspects of modern online life take place. The second element can be seen as the infrastructure, or foundation, on which this environment relies. This distinction will aid the exploration of freedom in cyberspace. As a consequence, for the rest of this research, the elements will be addressed as the (1) *digital environment,* and (2) the *infrastructure* which supports the digital environment. Combined, these elements form *cyberspace*.

Freedom in cyberspace according to non-domination

In the previous chapter, two main theories of freedom were identified. First, the negative account of freedom through Pettit's (1999) theory of freedom as non-domination. Second, the positive account of freedom through Nussbaum's (2000) capabilities approach. In this section, freedom in cyberspace will be explored through the lens of non-domination and in the next section, through the lens of the capabilities approach.

According to Pettit's theory, domination has to match the four conditions that were discussed earlier in this research. These are: (1) coercion of the body, will or the mind; (2) the interference has to carry adverse effects for the individual's situation; (3) the power has to be of arbitrary nature; (4) the dominating power must be *actually* capable to be exercised, not

merely a virtual capability. In this section, we explore what freedom in cyberspace would look like through the lens of the theory of non-domination. To do so, I will identify the conditions for domination in cyberspace. Through the identification of those conditions, I establish an idea of what the individual in cyberspace should be free *from*.

(1) First of all, the body does not play a role in cyberspace, but the will and mind certainly do. Society is increasingly becoming more digitalised, and a large share of social interaction, education, political engagement, and the management of personal finances are taking place digitally. In all of these aspects of life, the mind and will of an individual could, potentially, be coerced, and the individual's options can be negatively affected. A violation of the *integrity* of data matches this condition. To elaborate, if the *integrity* of the data online is compromised, then this will negatively affect the individual's choices. Since, if an individual receives a message from a trusted source, e.g. the government, and this message is altered by a malicious actor, then this individual is likely to be manipulated into making actions the individual would otherwise not make. Therefore, the threat to the *integrity* of data online matches the first condition of Pettit's theory.

(2) The interference has to affect the individual's situation adversely, this condition is more ambiguous in cyberspace. Take for example misinformation campaigns or "fake news", one can argue that the individual's thoughts are tampered with. However, the actor that instigated the misinformation campaigns can argue that it is not negative, but rather a diversification of opinions. In other words, this condition proves more ambiguous in cyberspace than in the physical world, however, the discussion of the capability approach in cyberspace will offer a solution.

(3) That the interference must be arbitrary, is a condition that is prevalent in cyberspace, as more often than not, cybercriminals remain unpunished. Due to the limits that a state actor experiences in cyberspace, proves it incredibly difficult to pursue justice in cyberspace and therefore malicious actors enjoy *de facto* arbitrary power. The third chapter provides a more profound analysis of the role of the state in cyberspace with relation to freedom in cyberspace.

(4) The capability to *actually* intervene is difficult to analyse in the digital environment, as technically speaking, every system could be infiltrated due to the presence of zero-day vulnerabilities. Zero-day vulnerabilities are weaknesses in a system that are thus far undiscovered, exploits utilising these vulnerabilities are therefore extremely effective and in fact, impossible to effectively protect against (Albanese et al., 2013, p. 3) At a later stage in this chapter, the actual vs. virtual capability will be further analysed. Having explored Pettit's conditions for a dominating power, a new set of conditions specific for cyberspace can be

introduced. These are: (1) a negative effect on an individual's mind or will, prominently through the compromise of the integrity of the information available online; (2) the interference, or capability, must have negative effects on the individual's situation, or alter its thoughts and politics without being aware of this; (3) the arbitrary power of the malicious actor is almost guaranteed in cyberspace, and therefore this condition can virtually be discarded; (4) the threat of a compromise must be real, the malicious actor must have the technical capabilities. To conclude, in Pettit's theory freedom is defined through the absence of domination. This domination comes in some sort of capacity to interfere, therefore, having identified the aforementioned conditions of a dominating interference in cyberspace, it becomes apparent that it is impossible to obtain complete absence of domination, rather I aim for the least amount of domination possible.

Freedom in cyberspace according to the capabilities approach

Nussbaum (2000) creates a conception of freedom through human functioning and capabilities. This conception fits cyberspace very well, although with a number of modifications and considerations. Nussbaum provides a list of capabilities that, if an individual would enjoy those capabilities, and does so with dignity, then the individual is considered to have a "worthy" human life (2000, pp. 7-10). However, the aim of this research is to explore what it means to be free in cyberspace. Therefore, in this section, the capabilities that are of relevance for cyberspace are discussed. These capabilities are then interpreted as to suit an individual's well-being in cyberspace. The goal is to create a sense of "digital capabilities" that lead to a certain degree of a "worthy digital life". This digital life does not equal a "worthy human life", the distinction is very important. Rather, the two work alongside each other. By having the capability to for example, move freely in the physical world, an individual can travel to a different continent, however, if the individual is then not able to move freely in cyberspace, e.g. engage socially with friends or family, the actual "freedom of movement" is somewhat undermined. Similarly, if one is able to engage socially with another that lives in another country, but subsequently is not able to meet the other individual physically, the "freedom of movement" in cyberspace is undermined to a degree, as by having the prospect of not being able to meet physically, one is discouraged from engaging socially with individuals from other continents or countries. As illustrated by the example, the exact relation between a "physical worthy life" and a "digital worthy life" is rather complex and could be the subject of an entire paper in itself. Therefore, in this paper we will consider the two versions as working in tandem.

Similarly, the "conventional" capabilities will offer a framework for the digital capabilities. Whether an individual enjoys having these digital capabilities will determine a large part of the individual's freedom in cyberspace, as I will explain in more detail in the final section of this chapter.

The conventional capabilities, simplified, are the following: natural life capability; healthy life capability; free movement capability; education, culture and independent thought capability; emotional capability; judgement capability; social capability; coexistence with nature capability; recreational capability; political participation capability and ownership capability (Nussbaum, 2000, pp. 77-80). When looking at cyberspace, the following eight capabilities, numbered in no particular order, are of relevance: (1) free movement capability; (2) education, culture, and independent thought capability; (3) emotional capability; (4) judgement capability; (5) social capability; (6) recreational capability; (7) political capability and (8) ownership capability.

(1) The capability to freely move oneself applies also in cyberspace, but does not concern the individual in physical form. Rather, it relates to an individual's possibility to move through the digital environment freely, without restrictions or borders. Since cyberspace is decentralised and borderless, individuals should not be concerned with restrictions on usage. Given, that the individual is legitimately authorised to access the date or source in question. To elaborate, an individual is not supposed to have access to one other's property, but is considered to have access at all times to data or sources that the individual has the legitimate claim to. For example, an individual should always be able to access the website of the government or of a national news station. Besides, certain networks that are necessary for one's social or professional functioning are ought to be accessible at all times. There are two exceptions to this, first, is malicious use, under which an individual can be banned from a certain network or website. Second, is the matter of property rights, which is elaborated upon in capability eight. (2) The capability to educate, culturally express, and think independently are of similar importance in cyberspace as in the physical world. For example, the spread of fake news or misinformation are negatively affecting the capability to think independently, due to relying on information that is created with the intent of influencing one's independent thought and choices (Tandoc Jr., 2019, p. 4). Furthermore, an individual ought to have the capability to pursue education and cultural experiences in cyberspace, without being limited. Both in the case of having to enter cyberspace to participate effectively, e.g. accessing online course materials and communication, or wanting to follow a course completely online, the capability has to be present. The same applies to cultural experiences, and "free" expression of ideas and

opinions. (3) The capability to engage in emotional relations online without another interfering or prohibiting the pursuit of emotional relations or expression. These relations can be of friendship, love or any other form of emotional connection. Furthermore, the expression of emotions online is also to be allowed. Individuals are allowed to portray and express their emotions online without restriction or judgement. With the exception of hate speech, abuse, or other malicious behaviour. (4) The capability to form judgement. Not only should individuals be capable of forming a conception of the "good" in the digital environment, but also should the individuals have the capability to judge what information online is to be trusted and what information is to be considered false. At times, this may be obviously beyond an individual's capability, however, the individual should have this capability to the furthest degree realisable. (5) The capability to socialise, this entails the mere capability to engage socially with others, without restraint. In cyberspace this is possible through messaging applications, social media, or (video)calling. (6) The capability to engage in recreational activities in cyberspace. This simply means not being restricted from pursuing activities of recreational nature in cyberspace. (7) The capability to engage and participate politically in cyberspace. An individual should be able to participate politically in the digital environment, this means unrestricted and not punished or treated differently for political engagement. For example, the individual holds the capability to form demonstrations or campaigns. Furthermore, similar to the capability of independent thought, an individual should not be restricted in engaging, expressing or participating with one's political beliefs. Of course, as long as it is not undemocratic or facilitating hate speech, discrimination, or violence. The details of what would be politically acceptable and not, falls outside of the scope of the research and therefore remains thus far purposefully ambiguous. (8) the capability to hold property, means that one is to be able to hold digital property such as websites, databases, personal info, multimedia, among many others. Therefore, property rules do exist, one is not allowed to enter another's property if that individual is not mandated access. This is best explained through the confidentiality aspect of the CIA-triad. In other words, it is not allowed for an individual to access data that is within the property of another entity.

If an individual is able to enjoy a certain degree of these capabilities then this individual is considered to have a decent digital functioning. A crucial part of Nussbaum's conception is that all of these capabilities apply to individuals, and not to groups or systems. Therefore, the individualistic approach of Nussbaum actually fits the cyberspace very well due to the limited role of an authority in cyberspace.

A conception of freedom in cyberspace

Both theories pose a compelling account of freedom, and the theories prove to be applicable, even to a complex domain such as cyberspace. However, neither non-domination, nor the capabilities approach are translated seamlessly into cyberspace. As a solution, the two conceptions, with their discussed interpretations, can be combined into a comprehensive conception for freedom in cyberspace. Interestingly, the capability approach provides us with a certain "situation" that ought to be protected from threats that undermine this situation. That situation is defined by the capabilities of the individual. On the other hand, through the non-domination theory relational freedom is considered. Namely, that by minimising the degree of freedom is increased, according to Pettit. When combined, these theories offer a comprehensive broad understanding of freedom.

In sum, the conception of freedom in cyberspace can be structured as follows: *if an individual enjoys digital capabilities and the domination that the individual is subject to is minimised to the furthest extent feasible, then the individual can be considered "free" in cyberspace.* This conception, I would like to call "cyber freedom" and throughout this research "cyber freedom" and "freedom in cyberspace" will be used synonymously.

This definition can be structured in two main elements: (1) enjoy digital capabilities; (2) minimisation of domination. As discussed earlier, the digital capabilities are: (1) free movement capability; (2) education, culture, and independent thought capability; (3) emotional capability; (4) judgement capability; (5) social capability; (6) recreational capability; (7) political capability and (8) ownership capability. To be free, means that an individual is able to have these capabilities. Each individual is free to use, or not use capabilities as they wish.

Chapter III

Thus far, in this research, cyber freedom has remained within the limits of an academic discussion and considered merely the individual. To go beyond that, this chapter will delve deeper into how cyber freedom in society can be achieved, and what such cyber freedom would look like in society. In the first section, the meaning of cyber freedom in society is discussed. Secondly, the role of cybersecurity, as an enabling means, will be examined in the second section. Lastly, the third section will examine the role the state should play in promoting, and protecting, cyber freedom.

Concepts such as "society" and "the state" are in themselves subjects for political philosophy, as a result, I will refrain here from a broad conceptual discussion about the meaning of these concepts. Rather, the abstractness of these concepts serve this chapter well, since the goal is not to make policy recommendations, but instead, create a normative idea of how cyber freedom would look like in society and what the role of the state is. For this research, I see "society" as a structure in which individuals operate and cooperate, where interactions take place. The aim of society is common prosperity and a just and equal standing of its members. The state takes the role of authority in society, and is responsible for the pursuit of the aforementioned aims. Through democracy, the leadership of the state would ideally reflect the interests of the *demos*, and therefore coincide with the societal aims. These ideas of society and the state are naively simplistic and idealistic, but for this normative discussion it serves its purpose well.

What does it mean to be free in cyberspace?

Cyber freedom, as conceptualised in the second chapter, is achieved through the possibility of the individual to enjoy digital capabilities and that the domination in the individual is subject to is minimised to the furthest extent feasible. Thus far, the conception of cyber freedom has focused solely at the individual. What would a society look like in which individuals are able to enjoy cyber freedom? The goal of this chapter then, is to extend the conceptualisation of cyber freedom to a society that has an adequate degree of cyber freedom. Since "freedom" remains an ideal, achieving "absolute freedom" is impossible, rather I strive for the maximum degree of freedom an individual, or in this case, the society, can obtain. In the next two sections, I will delve into the *measures* to protect or guarantee a certain status of freedom, therefore, in this section I merely explore what it means to be free in cyberspace in a

societal setting. The goal here is not to come with implications that directly could translate into law, rather, I aim to shape a normative account of how a society with a desirable degree of cyber freedom would look like.

Cyber freedom, as defined in this paper, consists of two main elements. A negative element, namely the minimisation of being subject to dominating power, and on the other hand, a positive element that introduces the notion, inspired by Nussbaum, of digital capabilities. When applying this conception to society, it becomes necessary to alter the conception slightly. In the context of society, the aim would be to minimise not being subject to dominating power, but rather, to minimise the presence of dominating relationships in society.

The eight digital capabilities are: (1) free movement capability; (2) education, culture, and independent thought capability; (3) emotional capability; (4) judgement capability; (5) social capability; (6) recreational capability; (7) political capability and (8) ownership capability. The aim is to strive to a desirable degree of digital capabilities, what would be the *desirable* degree? The primary objective is to provide every individual in the society with a basic degree of these capabilities. In other words, when distributing the resources that enable these capabilities, it is crucial to ensure that each capability is fulfilled to a certain extent. The division of the resources is not to be equal, or to be "fair", instead, in line with Nussbaum's thought, the sole driver behind the division of resources is to allocate them in such a way, that they would benefit the capabilities (Nussbaum, 2000, p. 71). In the last section of this chapter I will elaborate on the role of the state in allocating these resources. Thus far, I have regarded which capabilities members of society should *have*, however, there are also certain capabilities that members of society *should not* have. The capabilities that members of society should not have, are capabilities to interfere with others, or reduce the capabilities of others. For example, freedom of movement in cyberspace is limited by the ownership capability. Besides, certain digital capabilities include interaction with others, such as the emotional or recreational capability. With these interactions, it is important that both participants of the interaction do so willingly. In other words, one is not allowed to force or coerce another in having social contact. Thus, a permitted restriction on the capabilities is the mutual willingness when considering interactions. Similarly, when considering free movement in cyberspace, it is possible for an individual to be banned from a certain platform or website. If this were to happen, two important conditions apply: (1) the decision to ban a user has to serve to protect the capabilities of others; (2) the user that is banned, should have the possibility to receive a justification as well as the right to contest the decision. Crucially, the state will play an important role in maintaining an unbiased cyberspace, more on that in the last section of this chapter.

Having discussed what it means to be positively free in cyberspace, I now explore the other side of cyber freedom, the negative account of freedom. Whereas positive cyber freedom concerns a certain desirable "state" of freedom, negative cyber freedom instead addresses the relationships in cyberspace. How are relations between members of society shaped? The core argument of the Pettit's freedom as non-domination is that an individual is *unfree* if it finds itself in a dominating relationship. Relationships in cyberspace are complex, but actually are relatively similar to relationships in the physical world. However, the difference is that violence is replaced by cyber attacks, or the threat of a cyber attack. Unfortunately, every individual in cyberspace can be attacked and compromised, and it is impossible to be "completely" protected. That does not mean that it is impossible to be negatively free in cyberspace. Rather, it is worthwhile to analyse the relation between a (potentially) malicious actor in cyberspace and the potential victim. The balance of power lies in two aspects, (1) the technical ability of the malicious actor, and (2) the level of cybersecurity of the potential victim. It is virtually impossible for the potential victim to be aware of the level of cybersecurity that the malicious actor has. Therefore, the only aspect that remains in control of the potential victim is thus the level of cybersecurity. In the second chapter I will elaborate on the importance of cybersecurity for cyber freedom, however, for now it is important to be aware of the power dynamic that lies behind the *threat* of a cyber attack. Before I mentioned that everyone can be successfully attacked, then, why bother with increasing the level of cybersecurity? The solution lies in the motivation of the malicious actor, the vast majority of cyber attacks happen through the financial stimulus. However, by strengthening cybersecurity, the calculation for the malicious actor alters accordingly. At a certain point, it becomes simply not attractive enough for the hacker to waste its time on the potential victim, as it becomes more profitable to target another. Then, zooming out to the societal scope again, a problem appears. Namely, by strengthening cybersecurity the malicious actor simply targets another individual in society, and the problem is only moved from one individual to another. However, by continuously strengthening cybersecurity, which is a protracted process, the overall level of security in society becomes, on the whole, tighter and thus the incentive for hackers reduces.

In sum, what it means to be free in cyberspace is twofold. First, it means to enjoy the digital capabilities to the strongest degree feasible, while being ensured from checking all capabilities. Second, it concerns the continuous process of reducing power of malicious actors by strengthening cybersecurity. Together, this leads to a society that enjoys cyber freedom in a, generally speaking, treacherous cyber space.

Cybersecurity and freedom in cyberspace

Thus far I have discussed cyber freedom, however, the most common concept in cyberspace is "cybersecurity". Therefore, I will redefine what the role of cybersecurity is, not in the mere protection of digital information, but rather how it enables cyber freedom. Practices of cybersecurity are the means to secure the state of positive cyber freedom, as well as to serve in the pursuit of negative cyber freedom, through the protection of individuals in cyberspace. First, it is crucial to consider what cybersecurity really is.

Cybersecurity is a term that can be looked at from multiple perspectives. For this research I am less interested in the technological conception, which leans more towards "computer security" (Papakonstantinou, 2022, p. 3). Besides, a large quantity of literature is dedicated to the "national security" aspect of cybersecurity, considering the protection of essential infrastructure (Deibert, 2018, p. 411). While the protection of crucial infrastructure is essential to national security, it lies outside the scope and objective of this research. Besides, the "national security" focused approach is unfit in dealing with "human security" (Deibert, 2018, pp. 421-422).

Instead, I look at cybersecurity as a means to protect the individual's capabilities in the digital environment as well as minimise the capability to dominate within cyberspace. Note, that cybersecurity thus, is largely a means for the individual rather than for the society. This is due to the fact that I consider an open cyberspace, which results in the observation that it is impossible to collectively defend in cyberspace. What the state *can* do, will be considered in the next section.

Consequently, I aim to conceptualise cybersecurity as security from certain threats to one's positive freedom, i.e. digital capabilities, in cyberspace. However, the conception of cybersecurity also aims to enable individuals to reduce vulnerability to the capability to dominate by other actors in cyberspace. In sum, one can see cybersecurity as having two main aspects: the protection from threats to an individual's digital capabilities, as well as, the empowerment of individuals to be in possession of the tools and systems that reduce the threat to be dominated. As described earlier, by strengthening security, malicious action becomes less attractive. Therefore, the conceptualisation of cybersecurity for this research is as follows: *The protection of the individual's digital capabilities and the minimisation of the vulnerabilities in order to minimise the risk of domination.* Note that this conception of "cybersecurity" does not entail the discussion of technical controls or protective systems, this merely means the abstract meaning of it, being a means to achieve a certain situation of cyber freedom.

Does cybersecurity impair the cyber freedom of others? For this, I refer back to the theory of freedom as non-domination. Pettit provides the idea of antipower, namely the minimization of the capability of another to have power over the individual (Pettit, 1996, p. 588). In a conventional environment, Pettit argues that the simple maximisation of power to protect oneself does not lead to a more free situation, as the dominative power is merely relocated (p. 588). However, in cyberspace one can deploy protective measures, i.e. cybersecurity, in order to protect oneself better. Provided these measures are passive, for example the monitoring of network traffic, or the usage of antivirus-scanners, the individual does not increase their power in a way that it would be considered domination. If one individual has a sophisticated monitoring tool, that individual does not suddenly hold power over another individual. Therefore, I diverge from Pettit's traditional notion of antipower, as the provision of antipower through institutions seems to be essentially implausible due to the decentralised nature of cyberspace. Instead, the individual can increase one's protection regardless of others' freedom, as long as these measures are passive in nature. On the contrary, active measures exist, however due to the fundamentally different nature of these measures, these measures fall outside the scope of this research.

In sum, cybersecurity serves as the means to enhance negative freedom and protect positive freedom in cyberspace. In the next section the role of the state will be considered and elaborated upon.

The state and freedom in cyberspace

Lastly, I discuss the role of the state in facilitating cyber freedom in society. As discussed, the concept of the state is purposely left abstract. The role of the state in cyberspace is limited through the decentralised nature, as well as, the globalised nature of cyberspace. First of all, cyberspace is an intangible space in which the state cannot "patrol the streets". Besides, cyberspace does not *belong* or is under the control of the state, rather, the state is a mere actor in cyberspace. Secondly, cyberspace is globalised, threats can originate from any place in the world, which makes it nearly impossible for the state to pursue justice in light of criminal activities.

Then, what *can* the state do? I argue that the role of the state remains essential in facilitating freedom in cyberspace. Although through different manners than in the physical world, the state can foster cyber freedom in three main responsibilities: (1) awareness training; (2) mandatory certification schemes; (3) the allocation of resources to provide the digital

capabilities. First of all, one of the crucial responsibilities the state can take is to provide its population with adequate training on how to use cyberspace safely. The unsafe usage of cyberspace is one of the main drivers behind the success of cyber attacks. Through making the population more resilient, the dominating power of malicious actors is reduced, without the state itself becoming a dominating actor. Thus, conforming to the aforementioned concerns voiced by Pettit when enhancing antipower. Secondly, the state does not have full control over the devices used in cyberspace, but it can make it obligatory for all devices used within its *physical* territory to conform with certain security certificates. The neglect of secure configuration of devices is another main factor in the success of cyber attacks. By enforcing a mandatory certification scheme the state can create a safer society by reducing the vulnerabilities of individual's systems. This, however, would give the state a certain degree of control, which could potentially result in a relation of dominance. Therefore, the certification scheme should be assessed regularly by an independent commission in order to divide the power, and thus minimise the risk of a dominating relationship. Lastly, and more straightforward, the state should allocate sufficient resources to obtain the desirable degree of capabilities for its population. This also includes the maintenance and security of the infrastructural layer of cyberspace, which is necessary for proper usage of cyberspace.

Conclusion

In this research I aimed to answer the question: *what does it mean to be free in cyberspace?* And the answer to that question is provided for the individual in the second chapter, and subsequently elaborated upon in a societal setting in the third chapter. Through the thorough discussion of the two main theories of freedom used for this research, namely the account of freedom as non-domination and the capabilities theory, a comprehensive account of freedom in cyberspace, or cyber freedom, has been established. The established definition of cyber freedom is the following: *an individual can be considered "free" in cyberspace when the individual enjoys digital capabilities and the domination that the individual is subject to is minimised to the furthest extent feasible.* Subsequently, this conception of cyber freedom is applied to a societal setting, from which normative implications are drawn. First of all, the role of the state remains, as in the physical world, significant in facilitating cyber freedom. However, the role of the state shapes itself in a different manner, through the provision of education, certification schemes and the right allocation to serve the digital capabilities. On the other hand, cybersecurity serves as a *means* for the individual to protect positive cyber freedom and helps to foster negative cyber freedom. In society, the strengthening of cybersecurity results in collective gains, namely a more resilient society in cyberspace.

Academically speaking, the implications to draw lay in the direction of future research. Possibly, literature could build on the conception of cyber freedom established by this paper. Besides, future research is required into the more practical implications of the allocation of resources to serve the digital capabilities, and into the relation of conventional freedom and cyber freedom. Is this a casual relation, or a conditional relation?

This research is not without its limitations, first of all, the research is conducted through the lens of political philosophy and not through a technical analysis of the influence of individual cybersecurity measures on freedom. This could prove another avenue for future research. Secondly, as discussed in the third chapter, the analysis of the state and society is a purposely abstract one, and therefore it does not lead to concrete policy recommendations.

In sum, the aim of this research is to offer a broad exploration of freedom in cyberspace for both the individual and the society.

List of references

Albanese, M., Jajodia, S., A, S., & Wang, L. (2013). An efficient approach to assessing the risk of zero-day vulnerabilities. *In 2013 International Conference on Security and Cryptography*, 1-12.

Berlin, I. (1969). Two concepts of liberty. In *Four essays on liberty* (pp. 118-172). Oxford University Press.

Berlin, I. (2017). Two Concepts of Liberty. In D. Miller (Ed.), *Liberty Reader*. Taylor & Francis.

Carter, I. (2022). *Positive and Negative Liberty*. The Stanford Encyclopedia of Philosophy. Retrieved 12, 2022, from https://plato.stanford.edu/entries/liberty-positive-negative/

cyberspace - Glossary | CSRC. (2003). NIST Computer Security Resource Center. Retrieved December, 2022, from https://csrc.nist.gov/glossary/term/cyberspace

Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics & International Affairs*, *32*(4), 411-424.

Lane, M. (2018). *Ancient Political Philosophy*. Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/ancient-political/

Miller, D. (1998). *Political philosophy*. Taylor and Francis. 10.4324/9780415249126-S099-1

Miller, D. (2017). *Liberty Reader*. Taylor & Francis.

Nussbaum, M. C. (2000). Women's capabilities and social justice. *Journal of human development*, *1*(2), 219-247.

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state : The EU law path towards acknowledgement of a new right to cybersecurity? *computer law & security review*, *44*, 1-15.

Pettit, P. (1996). Freedom as antipower. *Ethics*, *106*(3), 576-604.

Pettit, P. (1997). *Republicanism: A theory of freedom and government*. Clarendon Press.

Pettit, P. (1999). *Republicanism: A Theory of Freedom and Government*. Oxford. https://doi.org/10.1093/0198296428.001.0001

Robeyns, I. A. M. (2016). *The capability approach.* he Stanford Encyclopedia of Philosophy. Retrieved 12, 2022, from https://plato.stanford.edu/entries/capability-approach/

Tandoc Jr., E. C. (2019). The facts of fake news: A research review. *Sociology Compass*, *13*(9), 1-9.