The Hybrid in the Cloud

A critical analysis of the practices of central actors within the European field of cloud computing

Marie Agerlin Olsen

Copenhagen Business School, 29 February 2016
Master's Thesis. MSc. in International Business and Politics
Advisor: Anna Leander, Professor (MSO), Dept. of Management, Politics, and Philosophy
Number of pages and characters: 74 / 165,355

Table of Contents

Abstract

Cloud computing[1] is by private companies and public institutions alike coined as the technological wonder that will dramatically boost economic productivity, and all are seeking ways to maximise the potential of 'the cloud'. One central change brought around by cloud computing is the significant growth of cross-border transfers data, which raises concerns relating to the regulation of data transfers to third countries, jurisdiction, responsibility, as well as the implications on the protection of the individual's right to privacy. Common to, and underlying, all these issues, however, are interlinkages of public and private actors; whilst the majority of the European cloud computing infrastructure is owned and controlled by private companies, a whole range of public institutions, private companies, industry organisations, civil society organisations, etc. seem to be concerned with cloud computing, and public actors are seen to increasingly seek control of this space. Within this network, however, public and private actors appear increasingly intertwined. It is the relation between public and private in the cloud as well as its implications that are under investigation in this thesis.

Situating the phenomenon of cloud computing in Europe within the theoretical framework of Bourdieu with field and *habitus* as central concepts allows for an analysis capturing the central actors, their practices, and the relations of power prevailing within the European field of cloud computing in order to eventually expose the hierarchies produced as a result. On the basis of this analysis, this thesis argues that within the European field of cloud computing resides a powerful yet obscure public/private hybrid, the actors, activities, purposes, and regulation of which are thoroughly entangled. The effects of the practices of this hybrid entail that security in and of the cloud is considered essential to the well functioning of the market, and that only those possessing the required, specialised technical skills get to speak on matters of cloud security. In this context the protection of individual privacy is continuously understated. Moreover, through the hybrid's successful proclamation of the commitment to transparency, regarding the handling and use of data stored in the cloud, civil society organisations advocating civilian rights to privacy are left entirely without a voice. The absence of these organisations within the field is striking.

[1] See Appendix 1 for a brief explanation of the technology.
[2] http://www.news.com.au/technology/online/security/world-war-iii-will-be-cyber-war-that-is-could-win-

The power of the public/private hybrid is further amplified by the construction of the cloud as critical infrastructure and thus as an object whose security is absolutely necessary for – in this case – the *economic* functioning of society. Through this construction, concerns for privacy and the materialities to protect privacy in the cloud are placed outside the boundary drawn through the construction of the cloud as critical infrastructure.

Produced within this field is thus a hierarchy where the public/private hybrid, consisting of very specialised and technologically superior actors, prevails at the top, and where the individual as a bearer of rights to privacy ranks lowest. The public/private hybrid, through its enactment and misrecognition as divided into public *and* private, conceals this hierarchy making it appear normal or even invisible and thus constantly sustains the position of the individual and his or her rights to privacy and data protection.

Chapter 1. Introduction

Doomsday arguments about impending cyber war and devastating acts of cyber terrorism are inescapable in current debates on cyberspace. Most recently, John McAfee, the American software developer famous for creating the first commercial anti-virus programme, has stated that World War III will be come to pass in cyberspace, where terrorist organisations like Daesh have more advanced skills than countries in the West – including the US.[2] As McAfee puts it, we are living in *'…a doomsday machine of our own design, and it is only a matter of time before our weapons and technology are turned against us.'*[3] Countering this narrative are scholars like Thomas Rid, arguing that actual acts of cyber terrorism are highly unlikely considering the significant level of resources and specific intelligence required to develop and deploy a potentially destructive cyber weapon against a secured target.[4] Such an attack, he argues, would require the resources of a state actor. Yet, as evidenced in the statement by McAfee, the presumed threat from cyber attacks seems to generate something close to a permanent state of emergency through the construction of the cyber threat as radically new and radically dangerous. Today, the securitisation of cyberspace is practically a given.

Yet, what is of essence in debating cyber security[5] is not necessarily – or at least not limited to – the imminent threat of cyber attacks and the means necessary for the deployment and/or deterioration of cyber weapons. To commence a discussion of cyberspace focusing on the potential threat of cyber war or cyber terrorism to the detriment of the state as if national security were a principle that stands on its own and that trumps everything else, risks concealing deeper, more structural issues at stake resulting from recent developments in cyberspace.

---

[2] http://www.news.com.au/technology/online/security/world-war-iii-will-be-cyber-war-that-is-could-win-john-mcafee-says/news-story/45cff1e2e42f062e107183227fec1435

[3] Ibid.

[4] Rid (2011), pp. 27-29.

[5] This thesis shall adopt Dunn Cavelty's definition of cyber security defined as *'the set of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity, and availability of information.'* (Dunn Cavelty (2013), p. 105)

As opposed to other areas of security, it is not states but private companies who have traditionally been the ones in control of cyberspace, and as Dunn Cavelty argues, states must rely on private companies in the provision of security in and of cyberspace.[6] Private companies, that is, who consider the provision of commercial services in cyberspace, rather than the provision of security, as a core activity.[7] Traditionally, the provision of security has been the prerogative of the sovereign, Westphalian state, and privatisation of security has proved controversial through and through. Less so, apparently, concerning the private provision of cyber security. Increasingly, however, states are attempting to encroach upon this space, striving for control and authority herein.[8] Almost concomitantly, concerns are raised over state surveillance and individuals' rights to privacy. Although such concerns are not raised unwarranted – as shall indeed be demonstrated in this thesis – the question remains whether the case where personal data and information security are in the possession of private companies is any more desirable than the case where the state, an international organisation, or the EU is in authority.

Having said that, any claim concerning security, be it public or private, necessarily implies that something or someone is to be secured. Neither the threat nor that which is to be protected can ever be taken as a given. Indeed, as Bigo argues, *'[a]ny academic definition, which tries to stabilise the meaning of security is either naïve or politically motivated."*[9] Hence, when debating issues related to security in cyberspace, it is essential to ponder the question as to whom/what is to be secured and whom/what is deemed to constitute a threat, and in whose interest. As shall be argued in this thesis, however, in whose interest claims about security in cyberspace are forwarded, is neither necessarily distinctly public nor distinctly private. Rather, as Dunn Cavelty argues, a focus on public-private relations is central to capture how security as well as the responsibility to provide security in and of cyberspace is distributed between a variety of both public and private actors.[10]

[6] Dunn Cavelty (2016) in Abrahamsen and Leander (2016), p. 89.
[7] This specific question is not only relevant in relation to cyber security. Increasingly, private companies, whose core capacities do not necessarily involve the provision of security, are being let in charge of tasks traditionally pertaining to national security. The latest example is Sweden compelling all Danish companies transporting passengers from Denmark to Sweden to check passenger IDs and thereby effectively undertake border control.
[8] Dunn Cavelty (2016) in Abrahamsen and Leander (2016), p. 89.
[9] Bigo (2013) p. 126
[10] Dunn Cavelty (2009), p. 217.

In investigating this issue further and seeing as, the complexity of cyberspace and the multitude of actors operating within, require that analyses hereof focus on the characteristics and peculiarities of one distinct issue, focus in this thesis will be on the phenomenon of cloud computing in Europe.[11] The European field of cloud computing is chosen primarily because the majority of writings on cyber security and cyberspace in general are almost entirely US centred making for a very narrow focus in the debate. The European Commission defines cloud computing as *'...IT infrastructures, platforms, and software provided centrally and distributed to end users over a network.'*[12] In this way, computing power is made available on demand, data storage and processing are transferred to very large, remote data centres, and users can access this service from anywhere in the world with an Internet connection.[13] It is private companies, who own and control the majority of the cloud infrastructure and provide the majority of services, including security services to protect data stored in the cloud. However, as shall be demonstrated later on, major EU institutions are also concerned with security in and of the cloud, and with the 'Network and Information Security Services (NIS) Directive', the first legislation on cyber security to cover the entire EU, which was agreed on in December 2015, by the European Parliament, the Council, and the Commission, the cloud is now considered to constitute critical infrastructure.[14]

Yet, this thesis shall argue, that what is at stake here is not whether security in and of the cloud is provided by private companies or by states; rather, the issue lies in the conjunction of public and private. As shall be demonstrated, in the European field of cloud computing, public and private actors are intertwined in an intricate web of cooperation, competition, struggle, and interdependence. The largely concealed entanglement of these actors and their practices are of great consequence to the functioning of the field. Hence the central question addressed in this thesis is, *what is the nature of the relationship between central public and private actors within the European field of cloud computing, and what are the main manifestations and effects of their practices?*

[11] See Appendix 1 for a brief explanation and illustration of the technology.
[12] https://ec.europa.eu/digital-agenda/en/cloud
[13] European Commission (2012), p. 2.
[14] http://europa.eu/rapid/press-release_IP-15-6270_en.htm

In devising an answer to the research question, this thesis is structured into six additional chapters, each instrumental in reaching an answer to the research question. The following chapter shall constitute the foundation of the thesis, arguing for the theoretical framework adopted, which is anchored in the work of Pierre Bourdieu with field and *habitus* as central concepts. Adopting this framework will allow for an analysis capturing the central actors and their practices, the power relations prevailing within the European field of cloud computing, and the hierarchies they produce. It is by way of such an approach that it will be possible to uncover the relation between public and private and assess the manifestations and effects of their practices. Drawing on the theoretical findings of Chapter 2, Chapter 3 will argue for the way in which the methods applied in the subsequent analyses can capture these practices, relations of power, and hierarchies produced. To give a first indication of the relations between public and private actors within the area of cyber security, Chapter 4 will constitute a brief account of the way in which cyberspace has become of increasing concern within security communities, although private companies have traditionally been in control hereof. Drawing on these findings, the analysis in Chapter 5 will undertake a more graphic mapping of the positions of the actors involved in the European field of cloud computing, in order to identify central actors, the relations between them, and what capital they possess. To expose the taken-for-granted practices and logics prevailing within the field and synthesise the resulting field effects, the findings in Chapter 5 will be scrutinised further in chapter 6, which shall concentrate on the public-private relations uncovered and expose the manifestations, effects, and the hierarchies that are (re-)produced as a result, and thus make explicit the way in which some actors are rendered victims of the prevailing practices and how this position is constantly sustained. Finally, the thesis will be drawn to a close in Chapter 7 posing an answer to the research question as well as some further reflections on the conclusions reached.

Chapter 2. Theory

The central purpose of this chapter is to argue for the way in which the theories applied in this thesis will contribute to a better understanding of the practices of the central actors involved in European cloud computing. In order to make explicit the contribution of this thesis, the following section will cover a discussion of relevant literature on cyber security, focusing on the attention paid to the involvement of specific actors, including private company involvement as well as the relationship between public and private within the area of cyber security. Specifically, forwarded in this chapter will be the argument, that the insufficient focus on private company involvement in cyber security and, more importantly, the underlying insistence on the public/private dichotomy effectuates a misperception of the effects of practices related to cyber security that are simultaneously public and private. This point will be developed further throughout this thesis. Also identified in this section will be important caveats as well as points of convergence and difference in the selected literature.

Taking these conclusions as point of departure, the second section will demonstrate how the theoretical framework of Bourdieu can be applied to break down established dichotomies and capture the practices of the central actors involved in European cloud computing as well as their manifestations and effects.

2.1. The debate and actors in the cyber security literature

Cyber security, as a concept, was introduced on the post-Cold War agenda in the 1990s with especially American politicians and private companies arguing for the potentially devastating effects of digital technologies on modern societies.[15] Today, cyber security is listed as a central issue of national security in more and more states, and within contemporary debates on cyberspace and cyber security, to argue for the securitisation of cyberspace is practically a truism.

[15] Hansen & Nissenbaum (2009), p. 1155.

The current debate on cyberspace and cyber security can be roughly divided into three strains where arguments, predominantly, centre around: 1) the imminent threat emerging from cyberspace, e.g. in the form of cyber war or cyber terrorism with both government officials, politicians, private companies, and scholars alike warning of the risk of potentially devastating cyber attacks against critical infrastructures, upon which modern liberal societies inherently rely; 2) the inflation of the threat from cyberspace, with especially scholars like Brito and Watkins[16], as well as Rid[17] warning of the dangers of threat inflation, and arguing that actual cyber war as well as lethal acts of cyber terrorism are highly unlikely, considering the significant level of resources and specific intelligence required to develop and deploy a potentially destructive cyber weapon against just one secured target[18]; and 3) concerns for civil liberties in the face of increased government surveillance and control of the Internet, which were exacerbates following the revelations by Snowden concerning US surveillance programmes, including PRISM. Underlying all three strains of argument are discussions about which actors are being empowered in cyberspace and what role the state is playing: is the state becoming obsolete or gaining more control through cyberspace? Here, scholars like Salhi argue that state authority in cyberspace is not a matter of either/or; rather, state control should be measured by degree.[19] Cyberspace, he argues, may be borderless, the location from which cyberspace is accessed, however, is not. Individual access to cyberspace depends on the state from which cyberspace is sought accessed, whereby state authority is rendered central.[20]

The fact that cyberspace has been securitised – justifiably or not – and that states are scrambling to gain control of cyberspace is widely accepted within this debate, if not taken for granted. In connection with this and perhaps as a direct consequence, an explicit discussion as to what cyber *security* actually entails, as argued by Hansen and Nissenbaum, has been largely omitted within current Security Studies.[21]

[16] Brito & Watkins (2011), pp. 1-39.
[17] Rid (2012), pp. 5-32.
[18] Ibid. pp. 27-29.
[19] Salhi (2009), p. 211.
[20] Ibid. p. 211.
[21] Hansen and Nissenbaum (2009), p. 1156.

Applying the Copenhagen School of securitisation theory, Hansen and Nissenbaum aim to identify and situate cyber security as a distinct security sector.[22] To successfully coin cyberspace as an issue of security, i.e. an issue potentially subject to an existential threat, they argue, has significant political consequences in the sense that it consequently allows for exceptional measures in the name of its protection.

Hansen and Nissenbaum identify three security modalities, the acuteness and interplay between which are specific to the cyber security sector.[23] The first modality is *'hypersecuritisation',* denoting the way in which the discourse on cyber security is centred on inflated, often unrealised, disaster scenarios involving cascading threats and multiple dimensions of society, simultaneously. The imagery of disasters in rapid succession combined with the fact that very few of these disaster scenarios have ever happened generates a distinct equivocacy of cyber security. The second modality, *'everyday security practices',* refers to how actors capable of securitising, mobilise individuals' lived experiences, linking them to components of the disaster scenarios to make the hypersecuritisations appear more credible and, as a consequence, make individuals more invested in the protection of network security. The mere utterance of security is not sufficient to securitise and issue. Rather, it is has to be accepted by the relevant audience as an object subject to a severe threat and in urgent need of protection. More importantly, however, with the securitisation of everyday life, the individual is constituted as a potential threat or liability due to either simple carelessness, or inadvertence, or intentional malice. *'Technification',* as the last modality, refers to the technical expertise required to operate within the area of computer security. The largely hypothetical nature of a range of cyber threats as well as the pace of technological developments and resulting new means for attack, serve to warrant the authority and legitimacy of technical, expert knowledge. The concurrence of technification and securitisation within cyber security discourse serves to depoliticise the issue, as the political foundation of the securitisation come to be concealed through technical discourse. It is this move, Hansen and Nissenbaum argue, which makes cyber securitisations markedly powerful.[24]

[22] Hansen and Nissenbaum (2009), p. 1157.
[23] Ibid. p. 1163.
[24] Ibid. p. 1172.

Although Hansen and Nissenbaum argue for the presence of multiple discourses in contestation, they argue for the distinct way in which the referent objects of the cyber security sector, namely the network and the individual, are all connected to one entity, namely national and state security. The competition and struggle disappears. Consequently, they fail to capture the contestation and multiple discourses as they actually set out to do. Moreover, and as a result, this leads Hansen and Nissenbaum to completely fail to address the distinctive role of the private sector in the securitisation of cyberspace. This is because the concept of security, within the framework of the Copenhagen School, cannot be detached from state security.[25] As Buzan, Wæver and de Wilde argue *'[s]ecurity is an arena of competing actors, but it is a biased one in which the state is generally privileged as the actor historically endowed with security tasks and most adequately structured for this purpose."*[26] Whilst there is indeed truth in this statement, in the case of cyber security, however, the state is not the actor traditionally in control and may not be the most "adequately structured" for the provision of security within this domain. This is exactly where the sector of cyber security differs from other security sectors. We cannot assume a state-centric securitisation in this environment.

Intrinsic to any concept, however, Wæver argues, is a tradition, and a set of practices and connotations that are well established and from which a particular concept cannot be dissociated. This tradition, this history, is one of security understood in terms of conflicts and power politics between states as well as concerns of state sovereignty, i.e. the concept of security is state-centric. That is, although the concept can be linked to political processes and dynamics separate from the state per se, the concept of security cannot be separated from concerns of state security. In securitising certain issues, the state can exercise its 'exceptional right' and thereby obtain command of them.[27] To Wæver, what is essential when rethinking the concept of security is to assess the ways in which the traditional issues of threat, national security, and sovereignty transform under new circumstances, as well as the way in which states invoke these issues to gain control of sectors of society, which do not necessarily pertain to military issues.[28]

[25] Wæver (1998).
[26] Buzan, Wæver and de Wilde. 1998, pp. 36-37.
[27] Wæver (1998)
[28] Ibid.

Whilst this theoretical insight may indeed be of value when analysing the efforts made by states to gain control of cyberspace, aspects of security privatisation and the relation between public and private cannot be neglected as a consequence of an exclusive focus on state security.

However, critical, when examining matters relating to cyberspace is to focus neither entirely on private actors nor solely on state actors. As Eriksson and Giacomello argue, no single actor or type of actor enjoys complete authority in cyberspace, and private and public authority often overlaps.[29] The degree of authority and the significance of public and private actors vary across countries and dimensions of cyberspace.[30]

By much the same token, Dunn Cavelty argues that control in cyberspace should be conceptualised rather as an intricate web of governance structures formed by multiple, diverse actors engaging in activities in cyberspace. In an article focusing on control in cyberspace in relation to security threats to critical information infrastructures, Dunn Cavelty consequently argues that a focus on public-private relations is central to capture how security as well as the responsibility to provide security in and of cyberspace is indeed distributed between a variety of both public and private actors.[31] States, she argues, cannot provide security on their own and are required to share this responsibility with private actors possessing the necessary technical skills and often owning and operating the critical information infrastructure, which the state aims to secure. This is exactly the case in relation to cloud computing. In this environment, the state is in need of private actors in order to provide security for its own citizens, a task, which has traditionally been *the* fundamental responsibility of the nation state. Accordingly, states are increasingly seeking to integrate private actors in public-private partnerships to ensure critical infrastructure protection. Reaching consensus on the nature and/or existence of a given threat and what security and control measures are necessary to counter it, however, is difficult to reach, both between public and private actors as well as between government agencies – all in competition to define the nature of the problem at hand and hence the resulting policies to counter it.

[29] Eriksson and Giacomello (2009), p. 207.
[30] Ibid. p. 207.
[31] Dunn Cavelty (2009), p. 217.

Specifically, struggles persist over whose security is at stake: the state as whole, the individual, or a technical system? [32]

Whilst arguing convincingly for the importance of scrutinising public-private relations when analysing phenomena related to cyber security, Dunn Cavelty does not fully engage the nature of this relation and effectively treats the public and the private as entirely separate entities. Yet, In an article on US national intelligence, Leander warns of this exact distinction, arguing that it may risk obscuring and/or reproducing the power relations involved in the conjunction of public and private, and that what prevails in the case of US national intelligence is rather an obscure yet powerful form of public-private hybrid.[33] This hybrid is characterised by instances where logics and actors, traditionally considered distinctly public or distinctly private, overlap and become intertwined because in this hybrid, Leander contends, *'...the actors, their activities, their purposes, and their applicable rules and regulations turn out to be public and private simultaneously.'*[34] It is in refusing to accept the public/private divide as given that it will be possible to discern the effects of the overlapping and sometimes contradictory practices and logics resulting from this hybridity. In the following section, the importance of breaking down established dichotomies will be further explicated.

Feeding into this line of argument, however, Bauman, Bigo, Esteves, Guild, Jabri, Lyon and Walker have written a very comprehensive article on the impact of cyber mass surveillance on issues like national security, human rights, democracy, obedience and subjectivity, arguing that practices of cyber mass surveillance are carried out by networks of US and European actors that *'...are not only transnational but also hybrids between public and private actors.'*[35] The mechanism, through which a large bulk of the data is collected by intelligence services and the like, they argue, is exactly the cloud, where private companies store immense quantities of very precise data.[36] What this thesis will eventually demonstrate is that this public/private hybrid not only prevails in relation to mass surveillance in the cloud but within several aspects of cloud computing ranging from regulation to activities providing security in and of the cloud.

[32] Dunn Cavelty (2009), p. 218.
[33] Leander in Best & Gheciu (2014), pp. 197-220.
[34] Ibid. p. 199.
[35] Bauman et al. (2014), p.123.
[36] Ibid. p.123.

Hybridity, however, does not necessarily mean consensus and cooperation. Returning to Dunn Cavelty, it is important to note that according to her, although subject to struggle and competing interests, the solution on how to respond to a given threat is eventually found through consensus between the actors involved. However, in doing so, Dunn Cavelty omits to address the resistance of actors. More often than not there is not such thing as consensus between competing actors. Rather, a given solution and its effects are the products of resistance and of the power struggles between the actors involved. It is not consensus-based and it is not the strategy of someone or someone's speech act. In assuming consensus, one risks simply reproducing dominant structures to which resistance may indeed exist. As the following section will argue, what is important when attempting to understand the relations between actors in cyberspace is to uncover the relations of competition, resistance and hybridity and lastly the hierarchies produced hereof. Consequently, whilst largely agreeing with Dunn Cavelty on her arguments on the complexity of cyberspace and the need to understand the relations between public and private actors in this context, Dunn Cavelty does not fully engage the issue of struggle and resistance nor of the entanglement of public and private actors in securing cyberspace and what the actual effects of this are. This argument will be further explicated in the following section.

As evidenced in this section, aspects of public/private hybridity and the role of private companies are not thoroughly developed in large parts of the cyber security literature, primarily owing to narrow discussions on state-to-state relations, the destructiveness of cyber attacks, and the potential for cyber war. Even Hansen and Nissenbaum, who claim as one of their objectives to expose the multiple discourses operating in the securitisation of cyberspace, fail to address the role of companies and the relationship between public and private in providing security in cyberspace. One issue lies in their conception of security, where the discursive proclamations of urgency as well as the justification of exceptional measures, ultimately in the name of state security, are central. However, as shall be explicated in the following section, when adopting the theoretical framework of Bourdieu, what comes to matter when scrutinising aspects of security, in this case cyber security, is not the exceptional but rather the every-day practices of a range of actors, appearing natural, even taken for granted, yet determining the normalised security for some and insecurity for others.

This approach to the concept of security will prove central when uncovering the practices of central actors involved in cloud computing, the relations between them, and the manifestations and effects hereof.

2.2. The field and habitus

In order to capture the practices of the actors, in particular the companies, involved in European cloud computing and the resulting manifestations and effects, this thesis will make use of a theoretical framework anchored in the work of Pierre Bourdieu with field and *habitus* as central concepts.

According to Bourdieu, the social world is structured into social spheres, within which distinct logics and rules of the game prevail.[37] Field and habitus are concepts that can be applied as means to uncover the taken-for-granted logics within a field and the relations of power rooted in these logics. A field denotes a specific sphere of social interaction organised around a certain issue, which is considered of central importance and each field is characterised by particular practices and shared understandings of the world as well as specific understandings of what constitutes capital, i.e. a source of power. On the basis of their capital, some actors are able to shape these shared understandings and make them appear everyday-like and normal. This ability is denoted as symbolic power. As the practices and understandings come to appear everyday-like and taken-for-granted, the resulting relations of power seem natural or even invisible. As a result, power is concealed and resistance is reduced, thus sustaining the field.[38] It is the aim of this thesis to uncover such taken-for-granted logics and relations of power in order to determine their manifestations and effects within the European field of cloud computing.

Like a magnet, the field attracts actors with interests that are pertinent within that field. Every actor participating in the field, whether actively or unknowingly, is subject to the dominating structures of the field, i.e. the taken-for-granted logics and rules of the game. A field, however, is never static. Rather, it is a dynamic, constantly changing sphere of interaction, where struggle, resistance, and competition between actors prevail.

[37] The remainder of this section on the theoretical framework of Pierre Bourdieu is based on Leander in Denemark (2007), pp. 3255-3270.
[38] Note here, that resistance is reduced but never eliminated.

The rules of the game within a field as well as the relative value of various types of capital are constantly subjects of strategic struggles between actors, aiming to advance their positions within the field. Based on their capital, each actor operates and engages in power struggles from a specific position within the field and with specific understandings of the world. However, each individual actor does not determine this position, its own interests or how to advance these. These are determined by their *habitus* – i.e. their dispositions – and the field is the overarching mechanism structuring interactions between actors. In their competition to advance their own positions within the field, actors effectively struggle over the boundaries of the field by attempting to draw capital from other fields. This is because fields do not exist independently from each other; rather, they exist in context and the relative value of capital within each field and hence the relative position of each field is constantly an object of struggle. Hence, fields – like actors participating within each field – come to be hierarchically organised. This hierarchy too is in a constant state of flux. It is important to note this, as the ensuing analyses will only be able to provide a snapshot of the field of European cloud computing and the fields organised around it. This issue and ways to ameliorate it will be addressed in the methodology chapter.

Habitus results from the accumulated positions and dispositions of actors across fields whilst at the same time reproducing and shaping these positions and dispositions. *Habitus* is thus created in context, materials, through language, etc. *Habitus* is, however, neither the result of free will nor determined solely by structures, yet it constantly conditions and shapes actors' actions and ways of thinking. In this sense, *habitus* is reflected in actors' taken-for-granted understandings, attitudes, and ways of acting. Having said that, *habitus* is not to be confused with the concepts *socialisation* or *internalisation*. These are too interactionist. The concept of *habitus* emphasises contexts rather than social interaction.

Although *habitus* reflects all experience, it is partly field specific in the sense that it embodies and reproduces the rules and discourses prevailing in a particular field. Hence, actors moving between fields will need to adapt to the established rules within the new field if not to loose out in the struggle to gain position. Bourdieu, terms this initial maladjustment as *hysteresis*.

This particular point will prove important when analysing the way in which actors originally belonging within the field of national security make the transition into a field traditionally dominated by companies whose interests revolve around the optimisation of business models to maximise profits and not necessarily the provision of security, although one does not necessarily rule out the other. Moreover, a related question to be addressed is whether and/or what security logics are beginning to permeate the field with the entrance of professionals of security and what consequences this may have to the *habitus* within the field. To these issues, the thesis shall return. For now, it will suffice to simply place emphasis on the field-specificity of *habitus* and how *habitus* determines practices within a field, including the practices of the actors at the bottom of the social hierarchy. *Habitus* is what sustains the hierarchies and relations of power. At the bottom of the hierarchy within a field, are the individuals who are rendered victims of the prevailing rules of the game. However, their *habitus* too contributes to sustain these rules, and the targets are thus always complicit in the symbolic violence done to them. Hence, a central task of this thesis will be to make explicit the way in which some actors within the European field of cloud computing are rendered victims of the prevailing practices and how this position is continuously sustained.

As is becoming evident on account of the above considerations, what further aids in uncovering the power relations and hierarchies within the European field of cloud computing is the way in which Bourdieu's notions of field and *habitus* function to break down dichotomies that have traditionally been taken for granted such as structure/agency and material/ideational. In arguing for *habitus* to be constituted through accumulated positions and dispositions of actors across fields whilst at the same time reproducing and shaping these positions and dispositions, *habitus* becomes a *'structuring structure'*,[39] and structure is thus placed at the agency level, breaking down the structure/agency dichotomy. Realising this serves to make explicit that the field effects do not result from the conscious strategy of some all-powerful actor or from an alliance or consensus between actors. It is not a plot. Rather, the field effects result from the struggles and competition between actors as well as the points of convergence amongst them – all this on the basis of their habitus. It is not a conspiracy and it is not a system that is set up consciously.

[39] Leander in Denemark (2007), p. 3257.

The task in the ensuing analyses is therefore to expose the competition between actors and uncover the sources of capital within the European field of cloud computing, which actors are considered to possess this capital and who are not, how they each advance their own capital and position as well as the way in which these actors relate to each other.

Moreover, in breaking down dichotomies, this approach will move focus from the state-centric assumptions still dominating analyses within International Relations onto the wider spectrum of actors, be they public or private, and allow for analysis of instances where logics and actors of public and private seem to overlap and become intertwined. This is essential since we cannot, in a field traditionally dominated by private actors assume state authority and centrality. Neither can we assume the domination of private actors in a field where state actors are increasingly seeking control through an emphasis on the seemingly ever-vanquishing notion of security. As we shall see, public and private actors are in close cooperation on matters of cloud computing. Insisting on the orderly distinction between public and private is thus inutile, at best, whilst, at worst, it risks obscuring and/or reproducing the power relations involved in the conjunction of public and private.

Consequently, what this approach will facilitate is an analysis that breaks down established dichotomies and uncovers the taken-for-granted and everyday practices of actors operating within the European field of cloud computing in order to expose the concealed relations of power and domination prevailing within. It is by uncovering these field effects – i.e. the manifestations and effects of the practices of actors operating within and across fields – that it will be possible to assess what hierarchies are reproduced in the field through the positions and dispositions practices within result in. In short, applying Bourdieu's concepts of field and habitus will allow for an analysis capturing power relations prevailing within the European field of cloud computing and the hierarchies they produce.

2.3. (In)securitisation and the everyday practices of cyber security professionals

When addressing any issue related to security, however, it is important to recognise the fluidity of the concept, security. Drawing on the work of Bourdieu and other insights form political sociology and political theory, scholars of the Paris School[40] of security studies, argue for a governmental rationality of security and the existence of security fields dominated by security professionals engaging in the political construction of security.[41]

As Bigo argues, *'[a]ny academic definition, which tries to stabilize the meaning of security is either naïve or politically motivated.'*[42] What matters is the political act in arguing for the prevalence of a given threat, i.e. how, by whom, against whom, and in whose interest a threat is constructed as real. In attending to cyber security it is thus clear that such a concept should not be treated as if it were an object with one core meaning; rather, it is the result of processes involving practices of security.[43] Practices of security are ones carried out by actors, invoking the term 'security' for their justification.[44] Through these practices, some issues are securitised whilst others are insecuritised. The term (in)securitisation signals that security and insecurity are not opposites; the definition of insecurity, i.e. the threat, is intrinsic to the definition of security.[45]

Drawing on the concepts of field and *habitus,* Bigo argues that these processes of securitisation and insecuritisation operate through everyday practices and interactions of a range of actors in permanent competition to define that, which is worthy of protection, and that, which, in opposition, can be constituted as the abnormal – as the threat.[46] This focus on everyday practices is in direct opposition to scholars of the Copenhagen School who view securitisation as an exceptional discursive act.

[40] There are not necessarily clear-cut divisions between the different schools of thought within security studies; rather, the different theories deemed to pertain to the respective schools do overlap in certain respects and the division of these theories into distinct schools can be misleading. Nevertheless, this section will, treat the Copenhagen School and the Paris School as distinct theoretical frameworks in order to argue for the way in which the two strands of thought diverge and why use will be made of theory from the Paris School rather than the Copenhagen School.
[41] C.A.S.E. Collective (2006), pp. 448-449.
[42] Bigo (2013), p. 126.
[43] Ibid. p. 124.
[44] Ibid. p. 124.
[45] Balzacq, Basaran, Bigo, Guittet & Olsson (2010), p. 2.
[46] Bigo (2013), pp. 124-126.

However, what the application of field and *habitus* makes possible is to uncover the routine of security practices and the way in which security becomes the result of everyday practices (discursive *and* non-discursive) of security professionals in competition with each other as well as the conditions in society rendering certain securitising practices possible. The actors are striving to shape what is meant by security in order to render legitimate and demanded, their specific practices and their specific capital. In this process, lines are being drawn between the secure, the "normal", and the insecure, the source of fear, the "abnormal", i.e. that which is to be controlled or governed.[47] Accordingly, this process is inherently political; it is a means of governmentality. It is for this reason that the very notion of security must be questioned when theorising cyber security.

The actors in question are termed 'security professionals' because they attempt to monopolise the definition of the source of fear as well as that, which is necessary to combat this fear, by invoking their expert knowledge of security.[48] They do so in order to gain better standing in the power struggles prevailing between actors operating within a particular field.[49] Security is the product of their struggles as well as their points of convergence.

Hence, what is important is not only to uncover the relations of power and struggle within the field and the systems of meaning, i.e. the routinized, taken for granted practices, generated in this process, but the kind of securitisation that eventually results from these relations. What/whom is seen to constitute a source of fear, what/whom is worthy of protection, and how is this protection best provided and by whom? Who gets to speak of issues of cyber security in relation to cloud computing, and who does not? The answers to these questions may be entirely different from answers found in more traditional analyses falling within the framework of the Paris School of security studies, because the dominant actors involved may not consider security related aspects of cloud computing as their primary interest. Nevertheless, for reasons outlined above, the concept of security will have to be scrutinised.

[47] C.A.S.E. Collective (2006), p. 457.
[48] Balzacq, Basaran, Bigo, Guittet & Olsson (2010), p. 6.
[49] Ibid. pp. 3-7.

Chapter 3. Methodology

Undertaking an analysis based on the theoretical framework outlined in the previous chapter requires a specific methodological approach. The consistency of the conclusions reached in this thesis depends on a concurrence between the methods applied and the theoretical foundation of the thesis. Essential is to achieve coherence between the questions posed, the type of explanation, as well as how and why such an explanation may generate valid scientific knowledge on specific subject. The aim of this chapter is therefore to explicate the relationship between theory and method, and thus how the theoretical framework shall be operationalized. On this basis it will be possible to argue for the way in which this thesis can contribute to the generation of knowledge on the manifestations and effects of the practices in the European field of cloud computing. Inevitably, the methods applied will entail some shortfalls. These too will be explicated and sought amended to the greatest extent possible.

3.1. Explanatory programme

The central aim of this thesis is to uncover the main prevailing practices and taken-for-granted logics of central actors operating within (and across) the European field of cloud computing and the relationship between them in order to assess what hierarchies are produced and reproduced in the field as a result. This aim of explanation entails a certain understanding of what qualifies as an adequate explanation of phenomena in the world, whereby a valid explanation is considered one that succeeds in making a complex phenomenon comprehensible by translating that particular phenomenon into common-sense lines of reasoning.[50] This type of explanation is categorised, by Abbott, as the semantic explanatory programme, where the central objective of explanation is argued to be the reduction of the complexity of the given phenomena under investigation.[51] By making intelligible the manifestations and effects of the practices that appear everyday-like and taken-for-granted, the complexity of the field is reduced and it becomes possible to understand the relations of power and what hierarchies are produced in the field of European cloud computing.

[50] Abbott (2004) p. 9.
[51] Ibid. p. 9.

However, this approach does not make for an explanation that allows for an intervention into the functioning of the field.[52] It may be possible to identify the field effects but it is not possible to actively change them. Nor is it possible to account for exactly how they have changed or may change. To intervene into the functioning of a field and change a given phenomenon requires the prior identification of the necessary cause of that phenomenon, i.e. it has to be possible to predict phenomena in the social world on the basis of constant conjunctions. To put it simply: if 'a' is identified as a necessary cause for 'b' (when 'a' then 'b'), then 'b' can be predicted on the basis of 'a', and it is therefore possible to intervene in the phenomenon that is 'b' by manipulating 'a'. There are, however, as Lebow argues, no such constant conjunctions in the social world. [53] Social reality is differentiated and open ended, he argues. To the extent that they do exist, it is on so abstract a level that it has little, if any, explanatory value when the phenomenon under investigation is a specific field, characterised by distinct logics and rules of the game. This is not to argue that all arguments based on constant conjunctions take a form as simple as that of linear causation (when 'a' then 'b') or that causal arguments have no value; rather, it is to argue that such explanations have little relevance in a field, which, according to Bourdieu, is never static. In this thesis the phenomena under investigation is a dynamic, constantly changing sphere of interaction where struggle, resistance, and competition between actors prevail. The relative position of actors operating within this field, the relations of power between them, the systems of meaning prevailing within, as well as the position of each field in relation to others is in a constant state of flux.[54] Therefore, the analysis of the field cannot be based on constant conjunctions.

This line of reasoning also renders impertinent reductionist explanations relying on universalising moves that assume the ability to capture events in the world within one abstract law. Recall here how *habitus*, according to Bourdieu, is largely field-specific. Within each field exist distinct logics and distinct rules of the game. Moreover, as Dunn Cavelty argues, the complexity of cyberspace entails that reductionist explanations of cyberspace have little value; rather, analyses of cyberspace should focus on the characteristics and peculiarities of one distinct issue, but across varying settings.[55]

[52] Abbott (2004) p. 9.
[53] Lebow (2014) pp. 9-10.
[54] Leander in Denemark (2007), p. 3257.
[55] Dunn Cavelty (2009), pp. 214-215.

Hence, general arguments in the form of law-like explanations have no explanatory value in this context. In short, this thesis is neither action oriented, nor does it strive to produce some kind of formal knowledge; rather, the aim of this thesis is to reach an understanding of how one specific field functions.

These discussions on the inability to predict social phenomena on the basis of constant conjunctions and the relevance of general law-like explanations are rooted in arguments on what constitutes valid scientific knowledge. To this, the follow section shall attend.

3.2. Big debate

As alluded to above, the arguments on the validity of certain types of explanation and subsequently what kind of data is relevant and how this data can and should be collected and analysed are essentially founded in specific understandings of the nature of reality, i.e. in specific epistemological and ontological beliefs. That is, what are the units of knowledge and how do we acquire knowledge about them? As a necessary basis for arguing how the theoretical framework of this thesis can be operationalized is thus how and why the particular methods applied can capture reality. The question to be answered in this section is thus why the methods of this thesis constitute scientific knowledge and how it may contribute knowledge on the European field of cloud computing.

Underlying the above arguments against relying on prediction upon identified constant conjunctions, is an interpretivist view of the world, whereby it is held that social life cannot be decontextualized and measured; rather, things acquire meaning through interaction and context.[56] Recall, how *habitus*, according to Bourdieu is created in context, materials, through language, etc., and thus results from the accumulated positions and dispositions of actors across fields whilst at the same time reproducing and shaping these positions and dispositions.[57] To capture *habitus* the following chapters of this thesis are therefore concerned with the uncovering and interpretation of the actors' taken-for-granted understandings, attitudes, and ways of acting.

[56] Abbott (2004) p. 43.
[57] Leander in Denemark (2007), pp. 3256-3258.

Hence, in this thesis knowledge about the European field of cloud computing is achieved through interpretation of interactions between variables in the context within which the field exists, rather than through the identification of constant conjunctions.[58] This insistence on the importance of context and interpretation is not, however, to reject causal arguments altogether. Rather, it is to be mindful of the drawbacks associated with causation, especially when the object of analysis is the social world. In fact, the explanation of the practices and their effects within the European field of cloud computing will require an abstract analysis of actors' practices and taken-for-granted logics and their effects on the field. This is how the field effects may be uncovered. Simple narration cannot capture this. Nevertheless, the analysis in the following chapter will make use of narration. The reasoning behind this will be covered later on in this chapter. For now, it is important to stress that although causation is not rejected in this thesis, any causal arguments made will be context-dependent and made on the basis of interpretation, not some universally measurable observations.

Accordingly, it makes no sense to place an analysis of the European field of cloud computing within a positivist framework since, *habitus*, being largely field-specific and constructed through different positions and dispositions, cannot be extracted from context and rendered subject to some universal measure. Neither can a specific field and the practices prevailing within. The knowledge produced in this thesis is situated, not universal. Moreover, *habitus* places one additional demand on the researcher, since the researcher too has a specific *habitus* according to which action and interaction will be interpreted.[59] Interpretations of actors' practices within a field will thus inevitably be distorted by the researcher's own *habitus*. This means that the only way to achieve any scientific validity and to limit this distortion is for the researcher to constantly make obvious and be critical of own interpretations made.[60] In other words, the analysis has to be reflexive.

Lastly, it is important to touch on the traditional debate on agency and structure. Recall, how this dichotomy is precisely one that Bourdieu sought to break down by introducing *habitus* as a *"structuring structure".*[61]

[58] Abbott (2004) p. 43.
[59] Leander in Denemark (2007), p. 3258.
[60] Ibid. p. 3258.
[61] Ibid. p. 3257.

Although this theoretical framework may appear structuralist at first, the rules of the game within a field as well as the relative value of various types of capital are constantly subjects of strategic struggles between actors attempting to advance their own position. However, each actor does not determine its position, its own interests or how to advance these. These are determined by their *habitus* and the field is the overarching mechanism structuring interactions between actors. In this sense, attempting to distinguish between choice and constraint or agency and structure will not contribute toward producing relevant knowledge on the European field of cloud computing and the hierarchies produced herein. In this thesis, no ontological distinction will, therefore, be drawn between agency and structure.

3.3. Methods

Capturing the reality described above, and thus making comprehensible the European field of cloud computing, requires not only particular methods but also a particular timing of the methods applied in order to refrain – to the greatest extent possible – from imposing a self-invented structure onto the field. The collection and analysis of data will therefore be organised so that the analysis of the field in its entirety will follow as the final step of the enquiry, thus reducing the risk of conjuring up unfounded field effects.

Accordingly, as a first step in this analysis will be a brief account of the way in which cyberspace, although traditionally within the control of private corporations, has become of increasing concern within security communities. The aim of this analysis is to provide a first indication of the relations between public and private actors in relation to cyber security. This will aid in the second step of the analysis, which will take the form of a mapping of the positions of actors involved, aimed at uncovering what is considered to count as capital in the field, which actors possess it, how the actors are positioned in relation to each other and thus get a first grasp of the public-private relationship. This relationship will be further exposed through an analysis of the practices and logics of the public and private actors identified as central within the field.

The aim is to uncover the manifestations and effects of the practices and logics otherwise appearing normal and everyday-like in order to eventually make known the hierarchies produced and sustained as a result. Below follows a more detailed account of the particular methods applied at the three main steps of the analysis.

3.3.1. Cyber security: private dominance & the return of the public

This analysis will take the form of a small-N, record-based analysis, centring on major, high profile cyber attacks and the responses to these over time. Included in this analysis will be media reports of the events, political statements, journal articles, as well as international norms, regulation and institutions set up in the wake of major cyber attacks. Applying historical narration to account for the way in which cyberspace over the years has come to the centre of attention within security communities and how private and public actors have come to relate to each other is meant to serve as a means toward circumventing the inability of the semantic explanatory programme in accounting for change. Moreover, this analysis will give a first indication of the relationship between public and private within the area of cyber security.

One of the central points of critique towards methods employing the explanatory programme is that it provides no understanding of how things have changed or how they may change in the future. Semantic explanations only allow for a snap shot of the given phenomenon under investigation. In an analysis uncovering social hierarchies and repression, naturally, it is desirable to be capable of providing an account for how such hierarchies may change. Moreover, fields are in a constant state of flux as the relative strength of the actors within a field may change and, as a result, the prevailing logics will change. Yet, in social environments as complex as the European field of cloud computing, prediction is simply impossible. Hence, the following analyses will only provide an atemporal account of the European field of cloud computing.

3.3.2. Mapping the positions of actors

As a starting point toward reaching an understanding of the field effects of the European field of cloud computing, will be a mapping of the positions of actors operating within the field in order to determine the relations between these actors, what counts as capital, and which actors are deemed to possess it. The aim is to identify the central actors, the relationship between them, and what appear to be successful claims to authority. Having said that, neither the time, nor the resources available for this thesis allow for an empirical analysis as thorough as one required for a full-scale field analysis.

As a central piece in this mapping is a comprehensive, record-based empirical analysis mapping the central public and private actors involved, including the EU institutional and regulatory framework surrounding cloud computing. As a starting point of the analysis, the most recent EU regulation pertaining to cloud computing will be examined. Of concern when attempting to map the positions of actors within the field of European cloud computing are not only the actors themselves and the apparent relations between them, but also the laws and strategies regulating them. Not only will an investigation of these give an indication as to which actors are endowed with authority through such regulations but it will also serve as a means to identify which actors have taken part in their formulation and must therefore occupy a central place within the field. Additional to the analysis of regulation pertaining to cloud computing, the mapping of the actors involved will be done by examining the relations between them, investigating whether some of the same actors appear across different, policy bodies, stakeholder groups, and expert groups, such as ENISA's 'Permanent Stakeholders' Group', and the EC3's group of partners, as well as how and if the actors refer to each other. The logic of this analysis is that actors reappearing across these different groups and bodies must possess recognised authority and thus occupy a central place within the field. The aim is therefore to identify which actors possess authority, how actors confer authority onto others, and on what grounds. Doing so will aid in determining what is considered a source of power within the field and thus what counts as capital as well as which actors are deemed to possess it.

This type of analysis may appear very manual and time consuming as opposed to an analysis making use of software to conduct the mapping. The strength of this type of analysis, however, lies in the fact that it allows for the researcher to personally follow every step of the analysis and every connection detected between the actors under investigation. This aids the researcher in rendering this mapping subject to reflexivity and in being mindful of the risk of imposing a false structure onto the field. Nevertheless, as already argued, any researcher will have to accept some degree of theory dependence, mainly on the basis of one's own *habitus*, and a larger data set, which a software-based analysis would allow for, could admittedly reduce this dependence. However, the closeness to the data achieved through the more manual type of analysis allows for a very detailed and careful tracing of the actors and the relations between them, which eventually aids in thoroughly comprehending the actors, their activities, their logics, and eventually the field in its entirety.

3.3.1. Uncovering practices and their effects

The findings of the above analysis, mapping the positions of actors within the field and thus contributing toward an understanding of the relation between public and private, what counts as capital in the European field of cloud computing, and who is deemed to possess it, will function as the foundation upon which the following analysis will draw in uncovering the practices and taken-for-granted logics prevailing within the field as well as their effects and manifestations otherwise appearing normal and everyday-like. The aim is to eventually expose the hierarchies produced and sustained as a result.

In order to uncover what practices are dominant, the method applied in this analysis will be a small-N analysis applied to data from websites of actors identified as central within the field as well as formal EU records. These include, amongst others, the websites of the European Cybercrime Centre (EC3), the European Network and Information Security Agency (ENISA), Microsoft, and IBM, as well as records such as the NIS Directive and the Commission's strategy on cloud computing, 'Unleashing the potential of Cloud Computing in Europe'.

Conducting this small-N analysis will allow for the retainment of a substantial amount of information from each record and website whilst comparing the practices identified to search for more general patterns.[62]

The analysis will comprise an examination and comparison of the discourses applied by these actors as well as their activities and the proclaimed purposes of these activities. Comparing practices, including discourses, across actors operating within the European field of cloud computing will contribute toward making intelligible the prevailing practices and taken-for-granted logics dominating the field. The logic is that by uncovering these practices and systems of meaning appearing everyday-like and taken for granted in this field it becomes possible to capture their manifestations and effects, and the hierarchies that are (re-)produced as a result. The aim is to make explicit the way in which some actors are rendered victims of the prevailing practices and how this position is constantly sustained. Importantly, in doing so, it is not solely the practices of the actors appearing central in the field, which should be analysed; rather, it is essential to also investigate which actors appear less "prominent" and ponder the question as to who does not speak? That is, which actors are left without a voice in the European field of cloud computing? Which actors appear to be missing? It is essential to ask these questions as a means to lay bare the hierarchy produced through the practices in the field and to refrain from reproducing the hierarchies and taken-for-granted logics rather than exposing them.

3.4. Heuristic

The aim with this methodological approach, breaking down classical dichotomies and introducing a temporal as well as an abstract analysis within a largely semantic explanatory programme, is to open up the debate and the methods applied and thus facilitate a more critical and reflexive enquiry into the workings of the European field of cloud computing. This approach will not, however, contribute a means to change the effects of these workings.

[62] Abbott (2004) p. 22

Nevertheless, the approach of this thesis will contribute toward the generation of a deeper understanding of an aspect of cyber security and the relations of power and hierarchies and produced within the European field of cloud computing, through its focus on one specific issue within cyber security, namely cloud computing, and will not attempt at reductionist explanations of a field as complex as cyberspace.

Chapter 4. Cyber security: private dominance & the return of the public

The rules of the game and the relative value of different sources of capital are constantly subjects of strategic struggles between actors in the field. So far, however, the thesis has largely assumed that private corporations have traditionally been in control of cyberspace and that states are now struggling to gain authority within this field. Before moving on to an analysis of the field and practices of cyber security in relation to cloud computing, the task of this chapter is therefore to illustrate how private companies have been in control from the beginning and how the public is returning or even expanding within cyberspace. More importantly, doing so will aid as a first step in getting a grasp of the relation between public and private. This analysis is conducted primarily by examining a range of cyber attacks and the responses to these over time.

Since the invention of the Internet by the US military in the 1960s, cyberspace has largely been under the control of and shaped by private actors.[63] Indeed, then-President Clinton encouraged the private sector to take the lead in the development of cyberspace, arguing that government regulation of cyberspace should be avoided.[64] Yet, since the Internet is composed of multiple interconnected networks and multiple dimensions, is its impossible for one single actor – or type of actor – to exert absolute control over the Internet.[65] However, by the end of the Cold War, the idea that cyberspace may constitute a threat to national security began to materialise, particularly within political discussions in the US.[66] As early as 1993, John Arquilla and David Ronfeldt of the RAND Corporation declared that '[*c]yberwar is coming!*'[67] A few years later, politicians, the media, and private companies raised concerns over the risk of "electronic Pearl Harbours".[68] Soon after that the first cyber security policy agendas were drafted.

Despite the "doomsday-character" of these cyber war scenarios, cyber attacks, including carefully targeted cyber attacks, have indeed become more and more normal in situations of political dispute and violent conflict.[69]

---

[63] Dunn Cavelty (2008) p. 30.
[64] Eriksson and Giacomello (2009), p. 212.
[65] Ibid. p. 207.
[66] Hansen and Nissenbaum (2009), p. 1155.
[67] Arquilla and Ronfeldt (1993), p. 141.
[68] Hansen and Nissenbaum (2009), p. 1155.
[69] Dunn Cavelty (2015), p. 83.

One of the most well-know cyber attacks is the attack on Estonia in late April and early May 2007, in response to the government's removal of a Russian World War II memorial statue from the centre of Tallinn just two weeks prior to 9 May, a historic day for Russians, marking the Russian victory against Nazi Germany.[70] Russia and the large Russian-speaking minority in Estonia considered this a grave offence. Apart from violent street riots in Tallinn, the removal of the statue triggered a large wave of online attacks on public as well as private institutions in Estonia, peaking on 9 May, and lasting for almost three weeks in total. Starting as simple low-technology attacks such as ping floods and denial-of-service attacks, the attacks gradually grew more sophisticated and coordinated, employing botnets to dramatically increase the quantity of distributed denial-of-service attacks (DDoS).[71] Although Estonia suffered the – at the time – most severe DDoS attack ever, the effects of the attack remained minor and, as opposed to the street riots, had no violent consequences. Still, however, Estonian government officials were quick to compare the attacks with acts of warfare, describing the launch of the DDoS attack as *'a gathering of botnets like a gathering of armies'*,[72] and the Estonian government did in fact succeed in having the attack designated as an act of cyber *warfare*[73]. This notwithstanding that Estonia was never able to prove who was behind the attacks and had to retract statements claiming the Russian government as the perpetrator due to lack of evidence.[74] Moreover, even though the Estonian government never succeeded in extending Article 5 of the North Atlantic Treaty to cover the cyber attack, it did manage to have NATO establish the Cooperative Cyber Defence Centre of Excellence in Tallinn in the wake of the attack.[75] Along with the Centre, NATO created the Cyber Defence Management Authority tasked with coordinating the NATO-response in the case of cyber attacks against a member state or the organisation itself, signalling that NATO too considers critical the cyber threat.[76]

[70] On the cyber attack in Estonia: Rid (2012), pp. 11-13
[71] Rid (2012), pp. 11-12.
[72] Tim Espiner, 'Estonia's cyberattacks: lessons learned, a year on', ZDNet UK, 1 May 2008. As quoted in Rid (2012) p. 12.
[73] I will not go into the discussion as to why – to be perfectly frank – it appears irreverent to call the cyber attack in Estonia an instance of war. However, for an insightful and well-argued critique on the popular classification of cyber attacks as the one in Estonia as acts of warfare, see *'Cyber War Will Not Take Place'* by Thomas Rid.
[74] Rid (2012), p. 12.
[75] Ibid. p. 12.
[76] Center for Strategic and International Studies: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

Just one year later, another cyber attack occurred against a sovereign state, rendering proponents of the advent of cyber war increasingly outspoken. This attack took place in the context of the brief war between Georgia and Russia in August 2008, following the territorial dispute over South Ossetia.[77] The cyber attack, which started a few days prior to the military conflict, comprised three different kinds of attack: defacement of websites such as that of the Georgian ministry of foreign affairs and the national bank; denial-of-service attacks against public as well as private institutions and news media; and the distribution of malicious software designed to permit increased access for the attackers and to augment the amount of attacks.[78] In this case, too, the effects of the cyber attack were minor and non-violent. The most severe attacks comprise a denial-of-service attack of about six hours and a defacement of Georgian president Saakashvili's website with images comparing the president with Adolf Hitler.[79] Nevertheless, the cyber attack on Georgia was, as was the case with Estonia, swathed in warlike rhetoric by the Georgian government as well as the international press. Once more, Russian authorities were accused of perpetrating the attack, but again no conclusive evidence was found to support the accusation.

What this cyber attack and the events around it serve to illustrate is that, once again, cyber space has become a matter of national security and that states are increasingly involved in cyber aggression. What is important to note in this case, however, is that the Georgian government had recourse to Google for limiting the damaging effects of the cyber attack.[80] The denial of service attacks against government websites significantly hampered the government's ability to communicate its troubles and seek aid from the outside world. With the permission of Google, the Ministry of Foreign Affairs was able to establish a weblog on the company's online blogging platform, 'Blogger', to communicate internationally.[81]

[77] On the cyber attack in Georgia: Rid (2012), pp. 13-14.
[78] Rid (2012), p. 13-14.
[79] Ibid. p. 13.
[80] Ibid. p. 14.
[81] Ibid. p. 14.

The case of Georgia serves to illustrate how a sovereign state may be dependent on a private company to reattain its security. Moreover, in relation to critical infrastructure protection in and from cyberspace, states are increasingly dependent upon private companies owing to the fact that private companies own and control large parts of a state's critical infrastructure.[82] Having said that, cyber attacks are also often directed against private companies, which in some cases render the companies reliant on the aid of states to counter the attack.[83] The examples above are all of cyber attacks directed against states and – supposedly - perpetrated by states. However, the number of so-called 'Mega-Hacks' against private corporations has dramatically increased since 2004.[84] The aim of these attacks is normally to appropriate large amounts of data such as credit card information or consumer records. Of significant Mega-Hacks can be mentioned attacks against Boeing and the US Transportation Command.[85] Such cyber attacks, however, although directed against private corporations and presumably with criminal motivations, may still be deemed a threat to national security since a range of private companies are in charge of infrastructures critical to the functioning of modern, Western societies.[86]

This complex interdependence as well as the rise in (supposedly) state-led cyber attacks has led states to negotiate norms aimed at minimising and regulating aggression in and through cyberspace, and in the EU, the UN, and NATO, states have agreed to extend International Humanitarian Law to cover cyber operations.[87] Regarding the use of information and communication technology in the context of conflict and in recognition of the escalatory potential on conflicts of such technologies, states have established Transparency and Confidence-Building Measures (henceforth TCBMs) through the OSCE in December 2013.[88] The OSCE measures are voluntary and allow mainly for the exchange of information, since notification and observation measures are not incorporated in the measures.

[82] Dunn Cavelty (2009), pp. 216-217.
[83] An example is the ATP (advanced persistent threat) attack directed at a Danish company and some of its clients in 2014-2015, where the company had to ask for the assistance of the Centre for Cyber Security (part of the Danish Defence Intelligence Service) to counter the threat and help restore security. For more information, see the report on the incident published by the Centre for Cyber Security: 'King of Phantom – bagdør til hovedmålet', January 2016.
[84] Dunn Cavelty (2015), pp. 87-88.
[85] Ibid. p. 87.
[86] Ibid. p. 87.
[87] Ibid. pp. 90-91.
[88] Ibid. pp. 90-91.

More importantly, however, the *'Tallinn Manual on the International Law Applicable to Cyber Warfare'*, confirms the applicability of the concept of state sovereignty and related international principles in relation to actions in and through cyber space.[89] Several inter-governmental bodies back this claim.[90]

It is clear that the number of cyber attacks against both governmental and private targets have increased substantially over the past two decades, and the actors involved in perpetrating the attacks are not limited to governments but include private companies, activists, criminals, and terrorists as well. For years, insecurity in and through cyberspace has thus taken a significant place in political debate. Recently, however, the debate has become increasingly state centred stressing how more and more states are using cyberspace as a strategic tool in inter-state relations, the potential for cyber conflicts between states to escalate, as well as the risk of cyber terrorism.[91] Cyberspace is now unquestionably linked to national security. This reinforces the sentiment that cyberspace cannot be left to private actors. Yet, private actors are still dominant. This is not, however, and in concurrence with Eriksson and Giacomello, to reiterate the debate on whether the Westphalian nation-state is obsolete. What this chapter has served to illustrate is that, in contrast to more traditional issues of security, it is states rather than private actors who are increasingly attempting to enter and exert control over cyberspace. Companies as well as consumers and criminals have shaped this space, and state actors are now seen to depend on private actors in securing cyber space. In addition, however, companies are seen to rely on the aid of states to counter cyber attacks. This complex interdependence throws into question conventional assumptions within security studies and IR, more generally, on public-private relations as well as state authority and governance in relation to security. In using Bourdieu's framework, the task of the ensuing chapters is thus to avoid taking for granted such assumptions when analysing the European field of cloud computing and the hierarchies produced herein.

[89] Tallinn Manual on the International Law Applicable to Cyber Warfare (2013).
[90] Dunn Cavelty (2015), p. 91-92.
[91] Ibid. p. 82.

Moreover, it is important to be mindful of the hysteresis that may be experienced by actors originally belonging within the field of national security when making the transition into a field traditionally dominated by companies whose interests revolve around the optimisation of business models to maximise profits and not necessarily the provision of security. Moreover, a related question to be addressed is whether and/or what security logics are beginning to permeate the field with the entrance of states, and what consequences this may have on the *habitus* within the field. Essential here, is to ask the question as to whose security is at stake and what/whom is considered a threat. Who gets to speak on 'security in the cloud', and who is left silent?

Chapter 5. Mapping the European field of cloud computing

Having briefly illustrated the way in which private companies have traditionally been in control of cyberspace, how threats in and of cyberspace have now come to permeate concerns of national security prompting states to actively strive for control and authority within this space, and how a complex interdependence between public and private has come to increasingly prevail within cyberspace, it is now possible to centre on the specific European field of cloud computing to analyse what actors appear central, the prevailing practices and capital herein, whether logics of security have come to penetrate this field, and finally what the resulting manifestations and effects are. Still, however, we can assume neither the centrality of companies, nor the centrality of states. As previously argued, a distinction between public and private may also be mistaken. The first step in this analysis is, therefore, to identify the central actors and the relationship between them. Hence, the task of this chapter is to map the positions of actors operating within the field of European cloud computing whilst uncovering what is considered to count as capital and which actors are deemed to possess it.

5.1. Tracing actors in the European field of cloud computing

Instantly apparent when examining the framework of European cloud computing is the existence of a multitude of different actors and services, involving different stakeholders, EU bodies, and groups of experts, each with different but sometimes overlapping responsibilities. The specific European infrastructure of cloud computing is owned more or less entirely by private companies,[92] whereas the legal framework pertaining to cloud computing within the EU is developed and enforced by EU institutions – with, however, the participation of a number of private companies. The result is competition, negotiation and cooperation between public authorities concerning regulations and the use of cloud services; between private corporations to win contracts, to influence regulation, or to contract each other's services; and between public and private entities, especially concerning regulation. Below follows a more detailed account of this network.

[92] European Parliament (2012), p. 17.

The most recent EU regulation pertaining to cloud computing in Europe is The Network and Information Security Services (NIS) Directive, which was agreed on in December 2015, by the European Parliament, the Council and the Commission.[93] This is the first legislation on cyber security to cover the entire EU. [94] Parts of the proposed legislation will be directed at providers of cloud computing services, requiring them to notify relevant national authorities of security incidents and to establish *'appropriate security measures'*.[95] This comes as a result of the fact that 'the cloud', with this Directive, is constituted as critical infrastructure. Within this Directive, the European Network and Information Security Agency (henceforth, ENISA) will be granted a central role, including in relation to the notification of security incidents.[96]

European Union Network and Information Security Agency

ENISA is the agency responsible for network and information security within the EU. ENISA was established in 2004, where the Council and the European Parliament adopted Regulation (EC) No 460/2004, in order to ensure stronger network and information security, as well as awareness hereof, within the EU.[97] In view of the increasing challenges related to network and information security, stemming from rapid technological innovation and socioeconomic developments, ENISA was granted additional authority to provide best-practice examples and policy suggestions to the EU and its Member States.[98] ENISA's current role is thus to act as a centre of expertise in assisting the Commission, Member States, and business communities in policy development and in the prevention and response to issues of network and information security.[99] Specifically, ENISA undertakes technical, scientific tasks in relation to information security, and assists the Commission on technical aspects when developing or updating legislation pertaining to network and information security within the EU.[100] Moreover, a core objective for ENISA is to promote cooperation between private and public actors and the development of public-private partnerships.[101]

[93] Press release by the Commission: http://europa.eu/rapid/press-release_IP-15-6270_en.htm
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Regulation (EC) No 460/2004.
[98] Regulation (EU) No 526/2013.
[99] https://www.enisa.europa.eu/about-enisa
[100] Ibid.
[101] https://www.enisa.europa.eu/about-enisa/activities

ENISA's organisation consists of an Executive Director, a Management Board, an Executive Board and a Permanent Stakeholders' Group.[102] Interestingly, the Permanent Stakeholders' Group, representing relevant stakeholders and whose tasks involve advising the Executive Director and developing proposals for ENISA's work programme, consists primarily of industry representatives. In fact 50 % of the members are representatives from the industry whilst consumers and academics make up just 25 %, respectively.[103] A quick search of the names listed reveals that companies represented in the group include Symantec, one of the world's largest software companies providing security services, systems management, and storage[104]; IBM Security, the cyber security branch of IBM[105]; Airbus Defence & Space CyberSecurity, formerly Cassidian Cyber Security[106]; Microsoft[107]; Alcatel-Lucent, a provider of cloud technology[108]; and Intel Security who has recently acquired McAfee, specialising in online security services.[109] Moreover, industry associations like Belgian ISACA representing IT security professionals are also represented in the Permanent Stakeholders' Group.[110]

Each of the companies mentioned above either provides cloud-computing infrastructure, platforms, cloud-based services, or services to secure the cloud. Hence, whilst ENISA is a central agency within the EU regarding policy development and advice on security measures directed at providers of cloud computing and related security services, at the same time, such companies are ENISA's core partners. Not only does this signify the central position of private companies; perhaps more importantly, it signals the entanglement of public and private actors within the field.

[102] https://www.enisa.europa.eu/about-enisa/structure-organization
[103] ENISA Permanent Stakeholders' Group 2015-2017.
[104] https://www.symantec.com/about/government/relationscontacts.jsp
[105] https://ec.europa.eu/digital-agenda/en/nick-coleman
[106] https://www.enisa.europa.eu/media/multimedia/news-pictures/enisa-high-level-event-2012-brussels/tom-koehler.jpg/view
[107] https://blogs.microsoft.com/eupolicy/author/janneutze/
[108] https://www.linkedin.com/profile/view?id=ACgAAAATUa8Bb2_wuByr3iIQDUBj15GnB1WLFjk&authType=name&authToken=sDwr
[109] https://www.linkedin.com/in/cvishik
[110] http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/Marc-Vael-Elected-International-Vice-President.aspx

Howbeit, ENISA is not the only EU agency appearing central in relation to European cloud computing. Concerning law enforcement, the European Cyber Crime Centre (henceforth EC3) is in authority.[111] With the EU Internal Security strategy of 2010 – under which the establishment of EC3 was a priority – one of the three areas that the EC3 was tasked to concentrate on is cybercrimes and -attacks affecting information systems, including cloud services, within the EU.[112] This could have been perfectly reasonable had the EC3 been established within ENISA, since ENISA is responsible namely for network information security. Yet, the EC3 is established within EUROPOL and separately from ENISA, thus bringing into question the role of ENISA.

European Cybercrime Centre

The EC3 was set up in the wake of the EU Internal Security Strategy in 2013 with the proclaimed aim of reinforcing the EU law enforcement response to cybercrime and protecting EU citizens, governments, and businesses from the threat of cybercrime.[113] Specifically, focus in the EC3 is on organised cybercrime generating large profits such as online fraud, cybercrimes and/or cyber attacks against critical EU infrastructure and information systems, and cybercrimes inflicting severe suffering on the victims such as online sexual abuse.[114]

In carrying out this work, the EC3 depends on a range of partners, including ENISA. Interestingly, however, ENISA listed only as an EU Partner and not as part of the EC3's Advisory Group on Internet Security. This would have been perfectly logical since ENISA is the EU agency responsible for network and information security, which is exactly what the EC3 is tasked to protect from cybercrime. Again, the lines of authority between ENISA and the EC3 are not entirely clear. Moreover, the EC3's Advisory Group on Internet Security, which is made up almost entirely of companies, includes some of those same companies appearing within ENISA's Permanent Stakeholders' Group, namely Symantec, McAfee (Intel Security), and Microsoft.[115]

[111] European Parliament (2012), pp. 23-24.
[112] https://www.europol.europa.eu/ec3
[113] Ibid.
[114] Ibid.
[115] https://www.europol.europa.eu/ec3/useful-links

Also appearing on the list of advisors are Verizon[116], one of the world's largest communication technology companies providing cloud-services and wireless networks, Fox IT[117] specialising in a range of cyber security services, and Check Point Software Technologies Ltd.[118], which is one of the largest vendors of security solutions to prevent cyber attacks in the world.[119] Here too, the entanglement of private and public actors is evident, and beginning to reappear, are now a number of companies.

Private companies and industry organisations

Today, private companies own the majority of the European cloud-computing infrastructure.[120] Under the label Amazon Web Services (AWS), Amazon is the largest provider of cloud services, with a computing capacity ten times larger than the capacity of the other top 14 cloud companies combined.[121] Microsoft, Google, Verizon, and IBM, however, are also prominent providers and are increasingly gaining market shares.[122] As a further matter, only US companies currently offer large-scale commercial PaaS platforms[123], rendering European cloud providers, who are simply reselling US cloud services, dependant on US companies.[124] Here, it is important not to omit the economic aspects and commercial interests involved in the provision of cloud computing services. The International Data Corporation (IDC) has detected a growth rate of 35 % in the western European market for cloud services in the period from 2010 to 2015,[125] the value of the market for public cloud computing world wide reached nearly $70 billion in 2015, and over the course of the next four years the amount of new cloud-based services is estimated to triple in quantity.[126] Thus, the economic potential for private corporations investing in cloud infrastructure or cloud-based services is significant.

[116] http://www.verizon.com/about/
[117] https://www.fox-it.com/en/
[118] http://www.checkpoint.com/about-us/facts-a-glance/index.html
[119] https://www.europol.europa.eu/ec3/useful-links
[120] European Parliament (2012), p. 17.
[121] http://fortune.com/2015/05/19/amazon-tops-in-cloud/
[122] Ibid.
[123] For a definition and illustration of PaaS, se Appendix 1.
[124] European Parliament (2012), p. 14.
[125] ENISA (2012), p. 3.
[126] https://www.idc.com/getdoc.jsp?containerId=prUS25797415

Notably, private corporations occupy a central role in the most recent EU strategy on cloud computing, *'Unleashing the Potential of Cloud Computing in Europe'*, which was adopted by the European Commission in September 2012, with the aim to augment the employment of cloud computing across every economic sector within the EU.[127] A range of private companies have participated in the formulation of this strategy, and to implement it, the Commission has set up six working groups, namely the 'ETSI: Cloud Standards Coordination'; 'The Cloud Select Industry Group on Service Level Agreements'; 'The Cloud Select Industry Group on Code of Conduct'; 'The Cloud Select Industry Group on Certification Schemes'; 'Research: the Cloud Expert Group'; and 'The European Cloud Partnership'.[128] Representatives from the cloud computing industry are represented in each of the six working groups.

The ETSI: Cloud Standards Coordination group was launched in cooperation with the European Telecommunications Standards Institute (ETSI), which consists of representatives from over 50 different tech-companies, including Alcatel-Lucent, Microsoft, Intel, and IBM.[129] The standards coordination group consists of a wide variety of public authorities, including ENISA,[130] EuroCloud Europe[131], standards setting organisations, user associations and industry representatives. Leading this group, however, are Luis Jorge Romero, director of the ETSI[132]; Anders Kingstedt, senior advisor at Softarc, a Swedish company providing cloud services on Microsoft platforms[133]; Emmanuel Darmois, director of the cloud consultancy firm, CommLedge, and member of ETSI[134]; Bernd Becker, president of EuroCloud Europe and owner of Scout2Cloud Consulting Services[135]; and Wolfgang Ziegler, director of SBD IT Consulting GmbH, an Austrian IT company specialising in data processing and information security.[136]

[127] https://ec.europa.eu/digital-agenda/en/european-cloud-initiative
[128] Ibid.
[129] https://portal.etsi.org/Portal_common/TBChart.asp
[130] http://csc.etsi.org/phase1/organizations.html
[131] EuroCloud Europe is an independent non-profit organisation providing a network for knowledge sharing between customers and providers of cloud computing as well as research centres. The members of EuroCloud Europe include a large range of companies, including IBM. (http://www.eurocloud.org/about.html)
[132] https://ec.europa.eu/digital-agenda/en/luis-jorge-romero-digital-assembly-2015
[133] https://www.linkedin.com/company/softarc?trk=ppro_cprof
[134] https://www.commledge.com/about/motto.html
[135] https://www.linkedin.com/in/bbs2c
[136] https://www.linkedin.com/in/wolfgang-ziegler-9b9045b8

The Cloud Select Industry Group on Service Level Agreements, which is responsible for the development of standardised guidelines for service level agreements between professional cloud users and cloud providers, consists of representatives from the Commission and companies such as Intel, SAP[137], IBM, Microsoft, Atos[138], Dell, SoftLayer (purchased by IBM in 2013[139]), and Accenture.[140] Similar to the ETSI working group, EuroCloud Europe is also represented. Atos, Intel, Dell, Microsoft, SAP, and EuroCloud Europe are also included in the Cloud Select Industry Group on Code of Conduct, whose aim is to devise a code of conduct for providers of cloud computing.[141] Also included in this group is the Cloud Industry Forum, a non-profit corporation working to assist cloud-service providers in conforming to a code of practice, advocating the use of cloud-based services, and bringing closer together providers and consumers of cloud services.[142]

The majority of the aforementioned companies including Accenture, Atos, Amazon and SAP are on the steering board of The European Cloud Partnership,[143] whose central task is to promote the adoption of cloud-based services and devise common requirements for procurement in cloud computing,[144] and Accenture, EuroCloud Europe, IBM, SAP, Microsoft, Atos, Cloud Industry Forum, and Intel also appear within the Cloud Select Industry Group on Certification Schemes[145] tasked to compose a list of *'cloud relevant security certification schemes'*[146]. In this group ENISA has played a central role, since ENISA was the agency in charge of validating the findings of the group and providing the first proposed list of security certification schemes relevant for cloud computing, which was adopted by the group to apply in its work, and which was made – and later finalised – by ENISA.[147] Today, the final list of certification schemes is published on ENISA's website.

[137] SAP is a large German software corporation developing software for businesses to manage operations and customer relations. (http://www.sap.com/corporate-en/about.html).
[138] Atos is a large French corporation providing cloud services, cyber-security solutions, consulting, big data solutions, etc. (http://atos.net/en-us/home/we-are.html).
[139] http://fortune.com/2015/05/19/amazon-tops-in-cloud/
[140] Cloud Select Industry Group on Service Level Agreements (2013).
[141] Cloud Select Industry Group on Code of Conduct (2013).
[142] http://www.cloudindustryforum.org/content/about-cloud-industry-forum
[143] https://ec.europa.eu/digital-agenda/en/european-cloud-initiative
[144] Ibid.
[145] Cloud Select Industry Group on Certification Schemes (2013).
[146] https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-schemes
[147] Ibid.

Finally, whilst mainly academics and representatives from ENISA comprise the expert group on research, some of the same large corporations reappear, namely Microsoft, SAP, Alcatel-Lucent, Dell, and IBM.[148]

Now, even though Amazon, Google, and Verizon are large providers of cloud services, they do not appear to occupy central places within the field of European cloud computing. Rather, as evidenced above, companies reappearing within different working groups, EU agencies, and industry organisations include Microsoft, IBM, SAP, Intel, Symantec, Alcatel-Lucent, Accenture, and Atos. In addition to being members of many of the same industry organisations, working groups, etc., these companies are also linked together through more commercial ties. For instance, Atos lists amongst its partners SAP, Microsoft, Cisco, and IBM.[149] Specifically, Atos states that it is cooperating with partners in delivering services and solutions by integrating its partners' technological expertise or market leadership to complement its own capabilities,[150] and Atos' cloud services function on Microsoft's cloud infrastructure.[151] Similarly, Symantec develops security solutions for Microsoft's cloud-based Office 365,[152] SAP lists among its partners IBM, Atos, Bull (which is owned by Atos[153]), Intel, Microsoft, Accenture, Symantec, Amazon, and Cisco.[154] Symantec lists Cisco, IBM, Accenture, and Atos as central partners,[155] Accenture lists amongst its alliances Alcatel-Lucent,[156] and Intel, who has recently bought McAfee, lists Alcatel-Lucent, Amazon, Cisco, Google, and SoftLayer (IBM), amongst its partners.[157] Moreover, each of these corporations owns multiple smaller companies with which the other corporations also cooperate. In addition, the tendency for public-private partnerships naturally fosters commercial competition between the providers of cloud-computing services. The result is an intertwined, intricate network of entangled relations of competition, negotiation, and cooperation.

[148] Cloud Expert Group (2012), p. 3.
[149] http://atos.net/en-us/home/we-are/alliances.html
[150] Ibid.
[151] http://atos.net/en-us/home/we-are/alliances/microsoft.html
[152] https://www.symantec.com/solutions/office365
[153] http://atos.net/en-us/home/we-are.html
[154] http://go.sap.com/docs/download/2012/06/7618c9fc-157c-0010-82c7-eda71af511fa.pdf
[155] http://partnerlocator.symantec.com/partnersearch#
[156] https://www.accenture.com/dk-en/cmt-index
[157] http://www.mcafee.com/us/partners.aspx

As evidenced in this section, a wide range of actors currently operates within the field of European cloud computing. Currently, two separate EU bodies are responsible for the policy framework related to cloud computing, namely the EC3 and ENISA, the respective roles and responsibilities of which are unclear and sometimes overlapping. Each agency cooperates with different stakeholders and experts, however private companies such as Microsoft, Symantec, and Intel Security, are reappearing as partners of both ENISA and the EC3. Of other central companies identified were IBM, SAP, Alcatel-Lucent, Accenture, and Atos. These companies own the majority of the European cloud-computing infrastructure and are linked through relations of competition as well as cooperation. The competition is also evident between ENISA and the EC3 with one of the EC3's core tasks being the prevention of cybercrimes and/or cyber attacks against critical EU infrastructure and information systems, which in fact falls within ENISA's area of responsibility. This unclear division of authority could lead both agencies to loose standing in the field. Be that as it may, and although the analysis in this section has appeared to treat separately public institutions and private companies, becoming increasingly pronounced throughout this analysis is the intricate network of public and private actors intertwined through relations of competition, interdependence, negotiation and cooperation. Yet, as important as it is to uncover which actors and relations appear central within a field, equally vital is to ponder the question as to who does not. What has become apparent in this analysis is a striking absence of civil society organisations in a field where concerns for the individual's right to data protection and privacy would presumably be of great importance. This point will be investigated further in the following section.

Another peculiar matter identified when undertaking this mapping was that whereas it was straightforward to uncover which public organisations were involved in the work of the Commission, EC3, or ENISA, in some instances, it was surprisingly difficult to discern which companies were involved. At best, the names of industry representatives are listed but not which companies they represent. More commonly, however, it is simply stated that industry representatives have been involved without stating which ones.

This signifies a curious characteristic of a field where private companies, organisations, and public authorities are intertwined in an intricate network of overlapping domains and authority, but where the involvement of private companies is somewhat concealed in some instances. For now, however, the following section shall further trace the actors appearing central within the European field of cloud computing in order to identify what traits amongst these actors appear to be accepted as constitutive of capital within the field.

5.2. Tracing Capital in the European field of cloud computing

Having identified some of the central actors operating within the European field of cloud computing, the task of this section is make explicit their specific capital. It is on the basis of capital that some actors are capable of shaping shared understandings within the field, making them appear normal and everyday-like and thereby concealing the resulting relations of power. In this way, power is disguised and resistance reduced, thus sustaining the field and the hierarchies produced.

The logic of analysis in this section is that the actors identified as central in the preceding section must possess capital considered as fundamental in the field. Based namely on their capital, actors, according to Bourdieu, engage in power struggles from a specific position within that field. The central questions to pose here are what claim to authority each actor makes, and how/if do other actors in the field endow them with this authority. In doing so, it is important to be mindful of the fact that, according to Bourdieu, actors, in their struggle to advance their own positions within one field, effectively struggle over the boundaries of that field by attempting to draw capital from other fields. As argued earlier, with the entrance of states into and the securitisation of the wider field of cyberspace, logics of security may begin to permeate the field of European cloud computing. Of investigation in this section is therefore also, whether some actors make claims to authority applying traditional logics of security.

As evidenced in the previous section, ENISA and the EC3 are central public actors within the European field of cloud computing. With the EC3 being tasked with cybercrimes and/or cyber attacks against critical EU infrastructure and information systems,[158] the EC3 is effectively the EU body in charge of EU law enforcement in the cloud since cloud infrastructure has been coined as critical infrastructure with the NIS Directive.[159] It is with reference to the Directive and to the EU Internal Security Strategy that the EC3 claims authority. Additionally, however, the EC3 claims to possess leading expertise on the basis of their *...'highly specialised technical and forensic support capabilities'*, which serve to train and build the capacity of Member States and support their operations and investigations,[160] i.e. aiding to ensure security internally in the Member States. Somewhat countering the EC3, ENISA claims to possess wide technical expertise on cloud computing and positions itself as *'...the EU's response to the cyber security issues of the European Union, ... the 'pace-setter' for Information Security in Europe, and a centre of expertise.*[161] Indeed, with Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004 of 10 March 2014, ENISA is given the position as the EU's body of expertise in the area of network and information security.[162] Moreover, ENISA's guidelines and risk assessments concerning the use of cloud computing are applied across industries and EU Member States "going cloud".[163] Evidently, ENISA must possess some kind of capital. The question is, therefore, on the basis of what, apart from the reference to EU regulations, ENISA bases the claim to authority on? Specifically, ENISA claims to possess *'...very specific technical and scientific'* expertise in relation to cloud security and privacy in the cloud.[164] This expertise, ENISA argues, allows them to effectively advice all stakeholders on and provide an overview of all aspects of information security risks related to cloud computing.[165]

[158] https://www.europol.europa.eu/ec3
[159] http://europa.eu/rapid/press-release_IP-15-6270_en.htm
[160] https://www.europol.europa.eu/ec3
[161] https://www.enisa.europa.eu/about-enisa
[162] Regulation (EU) No 526/2013
[163] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing
[164] Ibid.
[165] Ibid.

It comes as no surprise that public authorities such as ENISA and the EC3 refer to issues of security, effectively drawing on capital from the field of national security, when making their claims to authority and expertise. However, in doing so, ENISA and the EC3 also make reference to their respective expert groups consisting mainly of private companies. Moreover, a central goal for ENISA is to promote public-private partnerships in securing the cloud.[166] As evidenced above, central companies like Microsoft, IBM, SAP, Alcatel-Lucent, Accenture, Atos, Symantec, and Intel Security own and manage the majority of the European cloud-computing infrastructure. The tendency for public authorities to cooperate with these companies in the regulation and use of cloud-computing services, serves to signify that the companies too must possess capabilities understood to constitute capital in the field, since authority is conferred onto them through their participation in different expert and stakeholder groups set up by public authorities such as ENISA, the EC3, and the Commission. Moreover, reports of the Commission, the EC3, and ENISA on cloud computing, and cyber security more generally, draw on information provided by private companies. For instance, ENISA sites Accenture twice in its report on the cloud as a critical information infrastructure.[167] This serves to signify that the capital of these companies may be based on claims to expertise and/or technical capability.

Namely claims to specialised, technical expertise and the ability to make the use of cloud computing simple and accessible are pronounced when examining each of the companies. IBM prides itself on *'...the world's most advanced analytics and cognitive computing toolbox',*[168] as well as their unique expertise to solve even the biggest challenges of any company with the help of cloud services,[169] and Alcatel-Lucent advertise themselves as cloud-specialists and their cloud platforms as the world's most advanced, arguing for the way in which they *'unite the best cloud technologies with high performance virtualised software.*[170] Similarly, Microsoft, with reference to its cloud platform 'Microsoft Azure' and its life-long experience with online services, claims technical expertise, specifically related to the development and provision of integrated cloud services.

[166] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing
[167] ENISA (2012), pp. 5 and 14.
[168] http://www.ibm.com/cloud-computing/index
[169] Ibid.
[170] https://www.alcatel-lucent.com/solutions/cloud-mobile

Referring to Gartner's Magic Quadrants, a widely referenced tool measuring the competitiveness of technology companies, Microsoft prides itself on being the only cloud provider, which is positioned as an industry leader within each of the cloud functions: infrastructure, platform, and software.[171] Unlike Microsoft and IBM, Atos bases its technical expertise not on the development of cloud technologies but on the construction of customised cloud architectures and strategies for other companies.[172] Lastly, owing to their innovations, SAP claims to be *'...at the centre of today's business and technology revolution.'*[173] What is interesting in the case of SAP, however, is that SAP describes its partners as *'certified SAP professionals'*[174], indicating that SAP, whilst granting authority to its partners, does so on the premise of SAP's own approval. Thereby SAP effectively ranks itself higher than its partners and grants itself authority through its own certifications.

Interestingly, common amongst these companies are claims to authority through the application of logics of security. This is in spite of the fact that it is only Symantec and Intel Security that actually specialise in security services. For instance, IBM accentuates trust and their ability to deliver *'unparalleled security'* in the cloud,[175] Atos emphasises their *'security discipline'* and *'information integrity,'*[176]Accenture advertises their expertise in data protection, risk assessment, and cloud-infrastructure security,[177] and Microsoft refers to their pronounced expertise in ensuring data protection and privacy in the cloud. Specifically, Microsoft claims to be industry-lead in data and privacy protection, and states how they were the first provider of cloud services to be recognised by EU data protection authorities for their commitment to EU privacy regulations.[178] Furthermore, Microsoft, once more emphasising trust and protection, draws attention to their specific expertise in protecting government data with reference to Microsoft Azure Government, which is a cloud platform developed specifically for the US government.[179]

[171] https://azure.microsoft.com/en-gb/overview/what-is-azure/
For an illustration of each cloud function, see Annex 1.
[172] http://atos.net/en-us/home/we-do/cloud.html
[173] http://www.sap.com/corporate-en/about.html
[174] http://www.sap.com/partners/search/index.html
[175] http://www.ibm.com/cloud-computing/index
[176] http://atos.net/en-us/home/we-do/cloud.html
[177] https://www.accenture.com/dk-en/service-cloud-security
[178] https://azure.microsoft.com/en-gb/overview/what-is-azure/
[179] https://azure.microsoft.com/en-gb/features/gov/

In this way, Microsoft makes reference to a distinctive logic of security, namely information security in relation to both governments and individuals, in their claim to expertise.

Somewhat related to this claim to authority based on the provision of data security and privacy, is the emphasis on transparency. According to Microsoft, for instance, costumers can access information on where their data is stored, how it is secured, under which circumstances it can be accessed and by whom,[180] Atos emphasises costumers' complete control of data,[181] and IBM advertises *'...total visibility and control'* of costumer data stored in the IBM cloud.[182] What is notable about the companies' claims to expertise in and commitment to transparency and data and privacy protection is the fact that no evidence was found in the previous section suggesting the centrality of civil society organisations advocating civil rights and privacy protection within the field of European cloud computing, the presence of which would seem natural in a field where concerns of data and privacy protection appear pronounced.

To this point the thesis shall return in the following chapter. For now it is important to draw attention to the way in which logics of security are applied as a means for actors to advance their own position within the field. In claiming the ability to protect governments, individuals, and companies alike, actors, whose core function is not the provision of security but rather the provision of commercialised technological services, strive to draw capital from a field, traditionally dominated by states, namely the field of national security. It may thus seem as if the attempt by public authorities to draw capital from the field of national security is not a sign of hysteresis; rather, it appears that security logics are beginning to permeate the field and may be affecting the *habitus* within the field.

[180] https://azure.microsoft.com/en-gb/support/trust-center/
[181] https://canopy-cloud.com/cloud-infrastructures/canopy-enterprise-private-cloud/use-cases#case-2
[182] http://www.ibm.com/cloud-computing/solutions

5.3. Sub conclusion

This chapter has served to identify the central actors within the European field of cloud computing and what traits are deemed to constitute capital herein. A mapping of the field identified as central actors the public authorities ENISA and the EC3, and private companies including Microsoft, IBM, SAP, Alcatel-Lucent, Accenture, Atos, Symantec, and Intel Security. Additionally, this mapping revealed an intricate network between these public and private actors, which are intertwined through relations of competition, interdependence, negotiation and cooperation. Common amongst these actors in their claims to authority and standing within the field were assertions of their very specialised, technical expertise and technological capacity. Prevailing amongst the companies was also a claim to long-term experience suggesting a means to position themselves above public actors who have only recently entered cyberspace.

Interestingly, claims to authority referring to distinct logics of security were detected amongst public as well as private actors, each effectively attempting to draw capital from the field of national security. This was to be expected in the case of public actors who, in general, are attempting to enter and assert themselves in cyberspace, which has traditionally fallen under the control of private companies. At first sight, drawing on the capital of security could be a sign of hysteresis. Yet, when private companies too are drawing on this capital, it would seem that capabilities related to security are indeed accepted as capital within the European field of cloud computing and that security logics are beginning to affect the *habitus* in the field.

In connection with this, what also became evident through these analyses was the apparent absence of civil society organisations in spite of the fact that central actors such as ENISA, Microsoft, and IBM accentuate the importance of data protection, privacy, and transparency in the cloud. At first glance, it could appear as if these actors are simply speaking in support of civil society organisations advocating the individual's right to privacy and data protection. Yet their absence indicates that, effectively, civil society organisations advocating civil rights and information security in the cloud are left entirely without a voice in the European field of cloud computing. This first clue as to the hierarchy produced in the field and the practices and systems of meaning related to the capital uncovered will be sought investigated further in the following section analysing the normalised practices and systems of meaning prevailing within the field, and subsequently the resulting manifestations and effects.

Chapter 6. Uncovering hierarchies in the European field of cloud computing

Through a mapping of the actors operating within the European field of cloud computing the previous chapter identified as central actors ENISA, the EC3, Microsoft, IBM, SAP, Alcatel-Lucent, Accenture, Atos, Symantec, and Intel Security as well as an intricate network between them, where these public and private actors are intertwined through relations of competition, interdependence, negotiation, and cooperation. Common amongst these actors' claims to authority in relation to cloud computing – as well as instances where authority was granted by one actor to another – were assertions of a very specialised, technical expertise and technological capacity, the ability to provide security in and of the cloud as well as the commitment to transparency regarding the use of data stored in the cloud. Hence, these traits appear to be recognised as a source of power, i.e. capital, within the field. According to Bourdieu, it is on the basis of this capital, that central actors are capable of shaping practices and shared understandings making them appear everyday-like and normal. This ability is what Bourdieu terms as symbolic power. As the practices and understandings come to appear everyday-like and taken for granted, the resulting relations of power and hierarchies seem natural or even entirely undetectable. As a result, power is concealed and resistance is reduced, thus sustaining the field and its effects.

Therefore, the central task of this chapter is to uncover the practices and systems of meaning appearing everyday-like and taken for granted in this field. This is essential in order to capture comprehensively the manifestations, effects, and the hierarchies that are (re-)produced as a result, and thus make explicit the way in which some actors are rendered victims of the prevailing practices and how this position is constantly sustained.

6.1. Tracing practices of the public/private hybrid

Throughout the previous chapter it became apparent that public and private actors are closely connected on matters of cloud computing. Furthermore, following the agreement between the European Parliament, the Council, and the Commission on the NIS Directive, the Commission now intends to instigate and formalise public-private partnerships on cyber security in mid-2016 as a part of the Digital Single Market Strategy put forward by the Commission in May 2015.[183] This is essential since we cannot, in a field traditionally dominated by private actors assume public authority and centrality. Neither can we assume the domination of private actors in a field where public actors are increasingly seeking control through an emphasis on the seemingly ever-vanquishing notion of security. Thus, the maintenance of any clear-cut distinction between public and private seems without foundation.

In an article on US national intelligence, Leander warns of this exact distinction, arguing that it may risk obscuring and/or (re-)producing the power relations involved in the conjunction of public and private, and that what prevails in the case of US national intelligence is rather an obscure yet powerful form of public/private hybrid.[184] To capture this hybrid, Leander argues, it is necessary to conceptualise the *"public as practice"*.[185] Leander defines the "public" as *'that recognized to be of common concern'*.[186] With the public/private hybrid, however, the public and the private is combined into *'a new kind of "public" practice.'*[187] This hybrid is characterised by instances where logics and actors, traditionally considered distinctly public or distinctly private, overlap and become intertwined, because in this hybrid, Leander contends, *'the actors, their activities, their purposes, and their applicable rules and regulations turn out to be public and private simultaneously.'*[188] When taking for granted the dichotomy between public and private the effects of the practices of this public/private hybrid are rendered entirely obscure.

[183] http://europa.eu/rapid/press-release_IP-15-6270_en.htm
[184] Leander in Best & Gheciu (2014), pp. 197-220.
[185] Ibid. p. 198.
[186] Ibid. p. 198.
[187] Ibid. p. 198.
[188] Ibid. p. 199.

In tracing the practices and logics of the central actors within the European field of cloud computing the entanglement of the actors and their activities as well as the purposes of these comes to materialise. The entanglement of the activities of ENISA, the EC3, and the private companies as well as the way in which actors within these organisations are involved simultaneously in public and private activities were evidenced in the foregoing chapter. Employees from the private companies were found to be deeply involved in the work of public institutions, serving in expert and stakeholder groups and taking part in the formulation and implementation of the European Cloud Computing Strategy. To give another example, prior to becoming the Executive Director of ENISA in 2009, Udo Helmbrecht worked for 18 years in the private sector, including 10 years for the German company Deutsche Aerospace AG, which was taken over by EADS in 2000.[189] Moreover, and specifically in the case of activities related to the provision security in and of the cloud, public and private activities appear largely similar in terms of the development of highly advanced technologies to ensure system and data protection. These instances where actors and their activities are simultaneously public and private are what Leander terms 'enmeshment'.[190]

It goes without saying that with this enmeshment of actors and their activities follows an enmeshment of the purposes of these activities. Rather than being distinctively separate, market and security logics constantly overlap within the European field of cloud computing. As in the case of US national intelligence, the companies involved in cloud computing, were in the previous chapter found to explicitly state that they operate according to a security rationale insisting on the importance of providing security in and of the could. For instance, Accenture was found to emphasise their expertise in data protection, risk assessment, and cloud-infrastructure security.[191] Simultaneously, however, the companies are involved in fierce market competition to sell their specific products in an increasingly valuable industry. Naturally, what is of demand in this market is not limited to cloud infrastructure, platforms and other services but also includes security services to secure the cloud as well as the data stored herein.

[189] https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director/20101118_CVUH.pdf
[190] Leander in Best & Gheciu (2014), p. 200.
[191] https://www.accenture.com/dk-en/service-cloud-security

In this sense, companies within the European field of cloud computing operate within a security order synchronously with operating within a market order in much the same way as private contractors were found to be part of both orders in the case of US national intelligence.[192]

As expected, the security rationale appears prominent within the work of the public institutions, including ENISA and the EC3, and with the NIS Directive, the cloud is now considered to constitute critical infrastructure and providers of cloud computing services will be required to notify relevant authorities in Member States in case of security incidents and to install appropriate security measures.[193] Focus within ENISA and EC3 is primarily centred on the cloud as critical infrastructure as well as the risks of cybercrime and cyber espionage following the increased use of cloud-computing services.[194] Little attention, however, is paid to the risk to consumer privacy should the cloud providers mismanage their data or should states unlawfully attempt to access this data. This is in spite of the significant commercial interests involved in the storing and selling of consumer information. Interestingly, however, evidence of these public institutions following a market rationale was also easily discernible. ENISA lists the '*smooth functioning of the Internal Market'* through operative networks as the key reason for ensuring network and information security.[195] On the Commission's website, issues pertaining to cloud computing, including the EU's overall strategy on cloud computing, are listed under 'Digital *economy'*, and the European strategy on cloud computing, 'Unleashing the potential of Cloud Computing in Europe' is adopted with the view of promoting *'...the rapid adoption of cloud computing in all sectors of the economy in order to boost productivity.'*[196] As demonstrated the purposes of these actors and their activities are thus also enmeshed and the traditional distinction between security and public on the one hand and market and private on the other is therefore entirely fallacious within the European field of cloud computing.

[192] Washington Post 2010 as referenced in Leander in Best & Gheciu (2014), p. 201.
[193] http://europa.eu/rapid/press-release_IP-15-6270_en.htm
[194] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing and https://www.europol.europa.eu/ec3
[195] https://www.enisa.europa.eu/about-enisa
[196] https://ec.europa.eu/digital-agenda/en/european-cloud-initiative

The last element that Leander identifies as enmeshed in the case of US national intelligence is regulation.[197] In the case of regulation pertaining to cloud computing, however, the enmeshment of public and private is less discernible. Yet, recall how the Commission, following the agreement with the European Parliament and the Council on the NIS Directive, now intends to instigate and formalise public-private partnerships on cyber security.[198] In this case, regulation effectively ties together public and private actors by institutionalising public-private partnerships. Moreover, in the case of the European strategy on cloud computing, the enmeshment of public and private actors effectively shapes regulation since both public and private actors were found to have taken part in the formulation as well as the subsequent implementation of the strategy.

Despite enmeshed regulation being less discernible in the European field of cloud computing, what has become apparent in this section is the existence of a public-private hybrid similar to the one identified by Leander in the case of US national intelligence, where the enmeshment of public and private determines not only the activities prevalent within the field but also the purposes of these and the way in which they are regulated. Insisting on a public-private divide cannot separate back out this enmeshment; rather this will serve only to obscure the hybrid and it is implications.[199] It is the implications of this hybrid and the practices within, which will be the focus of the final part of this analysis in order to make intelligible the manifestations and effects of the practices and eventually expose the resulting hierarchies.

What remains is now to ask what are the effects of the insistence on the centrality of highly specialised, scientific technological capabilities, the security logics and market logics alike applied as the purpose for the activities of the hybrid operating within the field of cloud computing, and the move of the cloud from a purely commercial technology into a security order where the cloud is now considered as critical infrastructure, and finally the proclamations by private companies about their commitment to transparency regarding the use of data stored in the cloud? All this exists in a field where a public-private hybrid seems to prevail and where civil society organisations are remarkably unnoticeable.

[197] Leander in Best & Gheciu (2014), pp. 202-203.
[198] http://europa.eu/rapid/press-release_IP-15-6270_en.htm
[199] Leander in Best & Gheciu (2014), p. 203.

6.2. The symbolic power of the public-private hybrid

Having exposed the public/private hybrid and the enmeshment of its actors, activities, purposes, and regulation, it is now possible to progress to an analysis of the effects of this hybrid and thus uncover the actual field effects of the European field of cloud computing. Hence, the last remaining step of this analysis is to make intelligible the manifestations and effects of the practices, appearing everyday-like and taken for granted within the field, in order to eventually expose the hierarchies produced through the hybrid-practices. The central conception applied to expose the manifestations and effects of the identified practices is the symbolic power of the public-private hybrid whereby practices and common understandings come to appear normal, thus naturalising or even concealing the power of hybridity. The symbolic power of the hybrid works through the (re-)organisation of common understandings.[200]

Bear in mind, however, that this is not to argue that the actors identified as central within the European field of cloud computing are masterminding the field according to some common consensus, consciously identified amongst them; rather, the power of this public/private hybrid resides in the elusiveness of the hybrid itself and in the presence and diffusion of specific considerations related to cloud computing across contexts.

The construction of the cloud as critical infrastructure to be secured is an example in point of this diffusion.[201] Throughout this analysis of the European field of cloud computing, security in and of the cloud has reappeared in claims to capital, activities, and as a purpose for these activities of public and private actors alike. Essential here, however, is to ask the question as to whose security is in fact at stake and what/whom is considered to constitute a threat. Who gets to speak on 'security in the cloud', and who is left silent? As Bigo argues, the meaning of the concept of security should never be stabilised; rather, what matters is the political act in arguing for the prevalence of a given threat, i.e. how, by whom, against whom, and in whose interest a threat is constructed as real.[202]

[200] Bourdieu (1990) as referenced in Leander in Best & Gheciu (2014), p. 214.
[201] Arguably, this diffusion could also be interpreted to flow in the opposite direction with the notion of critical infrastructure spreading across the context of cloud computing. Yet, as shall be demonstrated later on in this section it appears that cloud computing as a concept is also spreading across the context of the internal market.
[202] Bigo (2013), p. 126.

This question is particularly relevant in a field that has traditionally fallen outside the realm of security and where the central companies' core competence – ultimately – is the provision of commercial computing services and not necessarily the provision of security. In the previous section it was demonstrated how the private companies operated according to a security rationale and a market rationale simultaneously. Nevertheless, as Bigo et al. argue in the study for the European Parliament, *'[o]ne should, however, not lose sight of what is at stake in the emphasis placed on security provisions related to the cloud, and whose interests are thereby promoted.'*[203] Specifically, the industry selling Internet security solutions is increasingly profitable. The question is therefore, what *conception* of security the private companies apply and whether this differs from that of the public institutions. With the enmeshment of actors, activities, and purposes uncovered in the previous section it may be that public and private conceptions of security are perfectly similar, and indeed, no attention is paid to this question in Leander's article on US national intelligence; rather, the similarity between private and public conceptions of security is largely taken for granted. In this case, however, the definition of security cannot simply be stabilised nor can we assume that public and private definitions of security are similar.

One security concern discovered to appear prominent amongst ENISA, the Commission, the EC3, and the central companies alike is the protection of data stored in the cloud. Interestingly, amongst the public actors, the functioning of the internal market appears as a central objective for ensuring data in the cloud. For instance, ENISA lists the '*smooth functioning of the Internal Market'* through operative networks as the key reason for ensuring network and information security.[204] Similarly, the Commission's strategy on cloud computing, 'Unleashing the potential of Cloud Computing in Europe' is adopted with the view of promoting *'...the rapid adoption of cloud computing in all sectors of the economy in order to boost productivity.'*[205] The functioning of the internal market, that is, is a key concern in relation to cloud security and protection of data stored in the cloud.[206]

[203] European Parliament (2012), p. 20.
[204] https://www.enisa.europa.eu/about-enisa
[205] https://ec.europa.eu/digital-agenda/en/european-cloud-initiative
[206] Note how this is another example of the enmeshment of purposes.

Whilst ensuring that data is properly protected in the cloud may indeed serve as an incentive for companies *and* individual consumers to make use of cloud services and thus boost the internal market for cloud-based services, ENISA, the EC3, and the Commission largely understate the risk to individual privacy in the cloud. For instance, the risk to individual privacy is not mentioned even once in the ENISA Mission,[207] and ENISA lists cloud security under the category of 'Resilience of Networks and Services and Critical Information Infrastructure Protection' rather than 'Identity and Trust' where the issue of securing personal data is included.[208] Moreover, the Commission too seems to effectively detach cloud computing from concerns of security and data protection. Specifically, on the Commission's website, issues pertaining to cloud computing, including the EU's overall strategy on cloud computing, are listed under 'Digital economy', rather than 'Digital society' where issues of cyber security and privacy are included.[209] Furthermore, no concerns for the protection of the rights and freedom of EU citizens making use of cloud services are included as reasons for adopting the Commission's European cloud strategy.[210] Even the EC3 pays little attention to individual privacy, focusing rather on the individual as a victim of cybercrimes such as payment fraud, identity theft, and sexual exploitation, than as a bearer of rights to privacy.[211] [212] Not once does the EC3 include in its strategy or operations the risk to individual privacy stemming from the collection and/or mismanagement by public and private actors alike of personal data stored in the cloud. Moreover, due to the confusion regarding the respective roles of ENISA and the EC3, it is unclear which agency is in fact in charge of the protection of data and the fundamental rights of those individuals whose data is stored and processed in the cloud.

Hence, amongst public actors, concerns for data protection are tied largely to concerns for the functioning of the internal market and the adoption of cloud computing in order to boost the economy. The individual's right to privacy and data protection is widely understated.

[207] https://www.enisa.europa.eu/about-enisa/activities/mission
[208] https://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/data-protection-measures
[209] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
[210] Ibid.
[211] https://www.europol.europa.eu/ec3/cyber-operations
[212] Bigo et al also reached this conclusion in a study for the European Parliament conducted in 2012 (European Parliament (2012)). The study included in its recommendations to the EP, a stronger focus on the individual's right to privacy. Five years later, however, the situation seems unchanged.

To the extent that concerns for individual privacy are voiced amongst ENISA, the Commission, and the EC3, they are limited to instances of cybercrime and the protection of individual data that is already collected and stored with reference to concerns of national security and/or severe criminal activity.[213] Surprisingly little attention is paid to the protection of individual data from being unlawfully collected and stored by states or private companies.

In the previous chapter, however, it was found that some of the private companies, identified as central within the field, accentuated not only their commitment to data protection, arguing for their technical expertise in building high-tech software to protect data, but also a commitment to transparency regarding the use of data stored in the cloud. Microsoft advertises 'the trusted cloud' stating that *'...you know how your data is stored and accessed, and how we help secure it,'*[214] and IBM advertises *'...total visibility and control'* of costumer data stored in the IBM cloud.[215] Having said that, Microsoft openly states that they do disclose customers' data when legally required to do so, such as in cases related to US national security,[216] and that customers are only informed of the disclosure of information in cases where Microsoft is legally permitted to do so.[217] Moreover, as alluded to earlier, by arguing for the importance of transparency and by laying claim to authority with reference to their commitment to transparency, the companies effectively render dispensable the civil society organisations promoting the individual's right to privacy and data protection, whose absence in the field is remarkable. The result is a silencing of these organisations.

[213] See the Data Retention Directive, Directive 2006/24/EC, requiring the appropriate protection of personal data retained.
[214] https://azure.microsoft.com/en-gb/support/trust-center/
[215] http://www.ibm.com/cloud-computing/solutions
[216] This thesis will not cover the controversy of the cross-border transfer of EU citizens' private data, since this will require a comprehensive legal analysis. However, it should be mentioned, that only US companies currently offer large-scale commercial cloud platforms, rendering European cloud providers, who are simply reselling US cloud services, dependant on US companies and subject to their privacy policies. (European Parliament (2012), p. 14.) For more information on this, however, see the new agreement reached between the EU and US on 2 February 2016, which follows in the wake of the decision by the European Court of Justice to declare invalid the Safe Harbour Privacy Principles, regulating the transfer of data to non-EU countries, in October 2015, after determining that the principles failed to adequately protect the privacy of EU citizens.
[217] https://www.microsoft.com/en-us/TrustCenter/Transparency/default.aspx#_You_know_who

As a further matter, one should never underestimate the profitability of business models structured around the gathering, storing, and protection of data in an age where information is increasingly considered as a source of power and influence.

Hence, at first sight it may seem that a disconnect exists between the Commission, the EC3, and ENSIA on the one hand and the private companies on the other regarding the conception of cloud security, with the Commission and ENISA openly insisting on a market-based reasoning for securing the cloud and effectively downplaying the importance of individual data protection. Yet, market-logics and inattention to concerns for the individual's right to privacy were also detectable when examining the security logics applied amongst the private companies. Indeed, hybrids are exactly *'...social arrangements in their own right where contradictory systems co-exist and overlap.'*[218] This co-existence and contradiction produce paradoxes, which are otherwise difficult to grasp when applying the more linear understandings traditionally utilised in social analysis.[219] In both cases, it is apparent how the seemingly contradictory systems of market/private and public/security are indeed enmeshed within this public-private hybrid and how the individual and his or her rights to privacy and data protection are constantly placed at the bottom of the hierarchy.

The market-oriented security logic and the silencing of civil society organisations in relation to transparency is coupled with an insistence on the very specialised, technical and scientific skills required to provide security in the cloud. The emphasis on technology as key to expertise in relation to cloud security, constructs cloud security as technical and thus contributes to a depoliticisation of security in the cloud within a field where security is to serve the well functioning of the market, and where only those possessing the required, specialised technical skills get to speak on matters of cloud security.

Moreover, with the construction of the cloud to constitute critical infrastructure, the cloud is granted prominence as an object that is absolutely necessary for the functioning of society, thus amplifying the power of the actors who get to speak on matters of cloud security – which in this case are composed of the public/private hybrid.

[218] Teubner (2002), p. 331 as quoted in Leander in Best & Gheciu (2014), p. 212.
[219] Teubner (2011) as cited in Leander in Best & Gheciu (2014), p. 212.

In an article on the securitisation of critical infrastructure protection and the 'agential role' of infrastructure, Aradau argues for the way in which *'[t]he protection of critical infrastructure enacts particular distinctions between infrastructure and society, 'hard' things and 'soft' relations, human and non-human, matter and meaning.'*[220] As with the distinction between public and private, the distinction between the human and the non-human, Aradau argues, is a misconception immersed in relations of power since the practices drawing these distinctions effectively create a hierarchy of materialities and forms of exclusion.[221] Critical infrastructure, she argues, is not contrasting to humans; rather, it is constructed in the *intra-actions* between non-humans and humans, not in their distinction.[222] This construction of the cloud as critical infrastructure, as critical to the functioning of the market as well as public institutions dependant on the cloud in their daily work, effectively places the individual and his/her right to privacy and data protection at the bottom of the hierarchy. As Aradau argues, *'...the securitisation of critical infrastructure implies that some infrastructures become materialised as infrastructures to be protected at the national or European level, while other materialities are relegated outside the purview of government.'*[223] In the European field of cloud computing, the cloud comes to be constructed as critical infrastructure due to the economic consequences society would suffer should the cloud-infrastructure collapse. The individual's right to privacy is not necessarily at risk in such a scenario; rather, privacy is at risk if the data stored is mismanaged by states or by companies delivering cloud services. Yet, concerns for privacy and the materialities to protect privacy in the cloud lie outside the boundary drawn through the construction of the cloud as critical infrastructure.

Hence, it is by refusing to take as a given the distinctions between humans and non-humans and public and private, and by treating as enmeshed the actors, activities, purposes, and rules that it becomes possible to capture this hybrid and its implications on individual rights to privacy and data protection.

[220] Aradau (2010), p. 492.
[221] Ibid. p. 500.
[222] Ibid. p. 509.
[223] Ibid. p. 500.

In the context of cloud computing in Europe the protection of individual privacy is largely understated, perhaps even ignored as a result of the practices of the public/private hybrid. Discussions tend to focus on information infrastructure protection, the prevention of grave cybercrime such as child pornography, and threats to national security, and the organisations whose aim would be to speak for individual rights to privacy are left entirely without a voice. To the extent individual citizens are taken into consideration it rarely involves the individual as one possessing rights to privacy; rather it involves the individual as the victim of cybercrime. Moreover, the emphasis on technology as key to expertise in relation to cloud security, constructs cloud security as technical and thus contributes to a depoliticisation of security in the cloud within a field where security is to serve the well functioning of the market, and where only those possessing the required, specialised technical skills get to speak on matters of cloud security. The power of these actors is further amplified by the construction of the cloud as critical infrastructure and thus as an object whose security is absolutely necessary for the *economic* functioning of society. Furthermore, through this construction, concerns for privacy and the materialities to protect privacy in the cloud are placed outside the boundary drawn through the construction of the cloud as critical infrastructure. The result is a hierarchy where the public/private hybrid, consisting of specialised and technologically superior actors, prevails at the top and where the individual as a bearer of rights to privacy ranks lowest. The public/private hybrid, through its enactment and misrecognition as divided, conceals this hierarchy making it appear normal and thus constantly sustains the position of the individual and his or her rights to privacy and data protection.

Chapter 7. Conclusion

In closing, the central argument of this thesis, presenting an answer to the research question falls in three consecutive parts.

Firstly, it was argued that in dealing with an issue such as cloud computing, and cyber security more generally, it is vital not to take for granted the divide between public and private as it risks obscuring and (re-)producing the power relations in and hierarchies produced through the practices appearing everyday-like and normal if accepting as given the public/private dichotomy. Applying the theoretical framework of Bourdieu assists in breaking down established dichotomies and uncovering the taken-for-granted and everyday practices of actors within the European field of cloud computing in order to make intelligible the concealed relations of power and domination prevailing within and thus expose hierarchies produced within the field.

Secondly, confirming the argument above, a mapping of the European field of cloud computing revealed an intricate network between the central actors, ENISA, the EC3, Microsoft, IBM, SAP, Alcatel-Lucent, Accenture, Atos, Symantec, and Intel Security, where public and private actors are intertwined through relations of competition, interdependence, negotiation, and cooperation. The capital of these actors was found to be based primarily on their proclaimed highly specialised, technical expertise and technological capacity as well as their expertise in providing security in and of the cloud, thus effectively attempting to draw capital from the field of security. In connection with these claims to expertise in the provision of security it became evident that civil society organisations advocating civil rights and information security in the cloud are remarkably absent and left entirely without a voice in the European field of cloud computing with private companies speaking their cause instead in their attempt to gain standing within the field. This discovery gave a first indication of the hierarchy produced as a result of the field-practices.

Finally, by examining further the network between the public and private actors identified as central within the European field of cloud computing and the practices of these actors relating to their capital, it was found that this network was in fact rather a public/private hybrid, the actors, activities, purposes, and regulation of which were entirely enmeshed.

Through an investigation into the implications of this hybrid and its practices it was found that the effects of this public/private hybrid entail that cloud security is considered essential to the well functioning of the market, and that only those possessing the required, highly specialised technical skills get to speak on matters of cloud security. In this context the protection of individual privacy is continuously understated. Moreover, through the hybrid's successful proclamation of the commitment to transparency, civil society organisations, whose absence in the field is striking, are left without a voice. The power of this hybrid is further amplified by the construction of the cloud as critical infrastructure and thus as an object whose security is absolutely necessary for the *economic* functioning of society. Through this construction, concerns for privacy and the materialities to protect privacy in the cloud are placed outside the boundary drawn through the construction of the cloud as critical infrastructure. The *habitus* within this field thus entails a hierarchy where the public/private hybrid, consisting of specialised and technologically superior actors, prevails at the top and where the individual as a bearer of rights to privacy ranks lowest. The public/private hybrid, through its enactment and misrecognition as divided into public *and* private, conceals this hierarchy making it appear normal and thus constantly sustains the position of the individual and his or her rights to privacy and data protection.

7.1. Reflections and concluding remarks

Finally, *habitus* places one additional demand on the researcher, namely reflexivity, since any researcher also has a specific *habitus* according to which action and interaction will be interpreted.[224] Interpretations of actors' practices within a field will thus inevitably be distorted by the researcher's own *habitus*. This means that the only way to achieve scientific validity and to limit this distortion is for the researcher to constantly be critical of own interpretations made.[225] Whilst the proximity to the data in each step of the analysis achieved through the more manual field analysis applied in this thesis has made it easier to be mindful of and reflect on what interpretations were made and which paths in the analysis were chosen over others, it cannot circumvent entirely the distortive effects of *habitus.*

[224] Leander in Denemark (2007), p. 3258.
[225] Ibid. p. 3258.

Indeed, as already evident, it has proved difficult to refrain from (re-)producing the power of the public/private hybrid. Although a main objective of this thesis has been to illustrate the way in which public and private have been reconstituted in the European field of cloud computing through a reflexive approach, in treating as separate public and private actors, activities, and purposes throughout large parts of the analysis, the symbolic power of the hybrid is reproduced. This illustrates the inherent difficulty in escaping ones own situatedness and the categorisation effects that are intrinsic to it.[226]

Despite – and especially because of – this difficulty in capturing and refraining from reproducing the power of the public/private hybrid it is paramount to conduct further research on this hybrid to investigate its potential existence in and effect on other fields. Recall here how fields do not exist independently of each other. Similar hybrids may therefore exist in other fields, just as the effects of one hybrid may migrate from one field to another. Of pertinence, in this regard, could be an investigation into the workings of the recently established border controls between Denmark and Sweden, where transport companies are charged with carrying out identity checks of people travelling between Denmark and Sweden in order to stop paperless refugees from entering Sweden. The civil and human rights organisation EDRi has already coined the Swedish border control *'...a privacy nightmare for travellers.'*[227]

[226] Leander in Best & Gheciu (2014), p. 212.
[227] https://edri.org/swedish-border-control-becomes-a-privacy-nightmare-for-travellers/

Appendix

Appendix 1: cloud computing explained

Cloud computing

The European Commission defines cloud computing as *'...the storing, processing, and use of data on remotely located computers accessed over the Internet.'*[228] Cloud computing thereby allows for instant network access to a shared supply of computing resources, such as servers, applications, and networks, which can be configured and provisioned rapidly requiring minimal engagement by the provider of the service.[229]

Cloud functions

A cloud is normally categorised according to the type of service it provides, thus denoting a minimum of three technical cloud varieties.[230] The model below displays each of the three levels, illustrating how the two upper levels are built upon a lower level.

1. **Software-as-a-Service (SaaS)**: a SaaS cloud provides software applications available on demand, such as Office365, to remote users.
2. **Platform-as-a-Service (PaaS)**: a PaaS cloud provides a platform, where developers can build services and applications, which users can then access over the Internet – usually on a subscription basis, choosing only the functions they want to use.[231]
3. **Infrastructure-as-a-Service (IaaS)**: an IaaS cloud provides storage and computing resources, essentially through virtual machines.

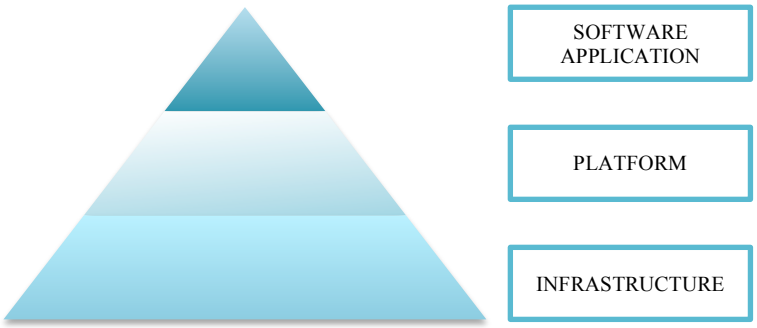

Figure 1: SPI model (source: Eurocloud Deutschland 2011)

Cloud categories

A further distinction is made between public, private, and hybrid clouds.[232]

- **Public cloud**: a public cloud can be accessed and used by anyone with an Internet connection.
- **Private cloud**: a private cloud is only accessible within a private network. One single institution controls all infrastructure and services in the private cloud. A separate institution, however, may own the cloud itself.
- **Hybrid cloud**: a cloud that has both public and private properties.

[228] European Commission (2012), p. 2.
[229] National Institute of Standards and Technology, USA (NIST).
[230] Description of cloud varieties: European Commission (2012), p. 2.
[231] The code of the application written for the platform does not have to be altered when distributed over thousands of machines in a datacentre and can thus easily adapt to and accommodate each new user's varying demands. The PaaS is, therefore, the only type of cloud, which allows for substantial scalability.
[232] On public, private, and hybrid clouds: EuroCloud Deutschland (2011), pp. 26-27.

Bibliography

Books

Abbott, Andrew (2004). *'Methods of Discovery: Heuristics of the Social Sciences',* W. W. Norton & Company, Inc.

Leander, Anna (2014). *'Understanding US National Intelligence: analysing practices to capture the chimera'* in Best, Jacqueline and Gheciu, Alexandra (2014). *'The Return of the Public in Global Governance',* Cambridge University Pres.

Bigo, Didier (2013). *'International Political Sociology',* in Williams, Paul D. (ed.) (2013). *'Security Studies: An Introduction',* New York: Routledge.

Buzan, Barry; Wæver, Ole and de Wilde, Jaap (1998). *'Security: A New Framework for Analysis'*, Boulder: Lynne Reinner.

Dunn Cavelty, Myriam (2016). *'Cyber-Security and Private Actors'*, in Abrahamsen, Rita and Leander, Anna (2016). *'Routledge Handbook of Private Security Studies'*, Routledge.

Leander, Anna (2007). *'Habitus and Field'* in Denemark, Robert A. (2007). *'The International Studies Encyclopaedia, Volume V'*, Wiley-Blackwell.

Lebow, Richard Ned (2014). *'Constructing Cause in International Relations'*, Cambridge University Press.

Teubner, Gunther (2002). *'Hybrid laws: constitutionalizing private governance networks.'* In *'Legality and Community',* edited by Robert Kagan and Kenneth Winston, pp. 311-31. Berkeley, CA: Berkeley Public Policy Press.

Wæver, Ole (1998). *'Securitization and Desecuritization'*, in Lipschutz, Ronnie (ed.) (1998). *'On Security'*, pp. 46-86. New York: Columbia University Press.

Institutional/governmental publications

Centre for Cyber Security (2016). *'King of Phantom – bagdør til hovedmålet'*, Copenhagen, January 2016. URL: https://fe-ddis.dk/cfcs/CFCSDocuments/Undersøgelsesrapport%20-%20KingOfPhantom.pdf [last accessed on 1 February 2016].

Cloud Expert Group (2012). *'A Roadmap for Advanced Cloud Technologies under H2020. Recommendations by the Cloud Expert Group',* edt. Schubert, Liz; Jeffery, Keith and Neidecker-Lutz, Burkhard, December 2012.

Cloud Select Industry Group on Certification Schemes (2013). *'Minutes of the meeting of the SIG-certification expert group',* Brussels, 21 February 2013. URL: https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-schemes [last accessed on 14 January 2016].

Cloud Select Industry Group on Code of Conduct (2013). *'Report of the first meeting of the Cloud Select Industry Group – Code of conduct Subgroup',* Brussels, 10 April 2013. URL: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Report%201.pdf [last accessed on 14 January 2016].

Cloud Select Industry Group on Service Level Agreements (2013). *'Report of the first meeting of the Cloud Select Industry Group – Service Level Agreements experts sub-group'*, Brussels, 21 February 2013. URL: https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements [last accessed on 14 January 2016].

EuroCloud Deutschland (2011). *'Guidelines, Cloud Computing. German Law, Data Protection & Compliance',* Cologne 2011.

European Commission (2015). *'Commission welcomes agreement to make EU online environment more secure'*, press release regarding the NIS Directive, Brussels, 8 December 2015. URL: http://europa.eu/rapid/press-release_IP-15-6270_en.htm [last accessed on 17 February 2016].

European Commission (2013). *'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union',* Brussels 7 February 2013.

European Commission (2012). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions: *'Unleashing the Potential of Cloud Computing in Europe',* COM(2012) 529 /2, Brussels, 27.09.2012.

European Network and Information Security Agency (ENISA) (2015), *'The Permanent Stakeholders' Group',* Term of office: March 2015 – September 2017. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/psg/members/list_alphabet20152017.pdf [last accessed on 12 January 2016].

European Network and Information Security Agency (ENISA) (2009), *Cloud computing: benefits, risks and recommendations for information security,* Heraklion, Greece, November 2009.

European Parliament (2012). *'Fighting Cyber Crime and Protecting Privacy in the Cloud',* Committee on Civil Liberties, Justice and Home Affairs, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs. PE 462.509, Brussels, October 2012.

National Institute of Standards and Technology, USA (NIST) (2011). *'The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology',* NIST, U.S. Department of Commerce, September 2011.

Sweeney, Eugene (rapporteur) (2011). *'Industry Recommendations to Vice President Neelie Kroes on the Orientation of a European Cloud Computing Strategy'*, Brussels: November 2011.

Journal articles

Aradau, Claudia (2010). *'Security That Matters: Critical Infrastructure and Objects of Protection'*, Security Dialogue, Vol. 41, No. 5, pp. 491-514.

Arquilla, John and Ronfeldt, David (1993). *'Cyberwar is Coming!',* Comparative Strategy, Vol. 12, No. 2, pp. 141-165.

Bak, Peter and Chen, Kan (1991). *'Self-Organized Criticality'*, Scientific American, January 1991.

Balzacq, Thierry; Basaran, Tugba; Bigo, Didier; Guittet, Emmanuel-Pierre and Olsson, Christian (2010), *'Security Practices'*, International Studies Encyclopaedia Online.

Bauman, Zygmunt; Bigo, Didier; Esteves, Paulo; Guild, Elspeth; Jabri, Vivienne; Lyon, David and Walker, R. B. J. (2014). *'After Snowden: Rethinking the Impact of Surveillance',* International Political Sociology (2014), Vol. 8, pp. 121-144.

C.A.S.E. Collective (2006). *'Critical Approaches to Security in Europe: A Networked Manifesto',* Security Dialogue, Vol. 37, No. 4, pp. 443-487.

Salhi, Hamoud (2009). *'The State Still Governs',* in Eriksson, Johan and Giampiero, Giacomello (2009). *'Who Controls the Internet? Beyond Obstinacy or Obsolescence of the State'*, International Studies Review, Vol. 11, pp. 205-230.

Dunn Cavelty, Myriam (2015). *'The Normalization of Cyber-International Relations'*, Strategic Trends 2015. Center for Security Studies, ETH Zurich, pp. 81-98.

Dunn Cavelty, Myriam (2009). *'National Security and the Internet: Distributed Security through Distributed Responsibility',* in Eriksson, Johan and Giampiero, Giacomello (2009). *'Who Controls the Internet? Beyond Obstinacy or Obsolescence of the State'*, International Studies Review, Vol. 11, pp. 205-230.

Eriksson, Johan and Giampiero, Giacomello (2009). *'Who Controls the Internet? Beyond Obstinacy or Obsolescence of the State'*, International Studies Review, Vol. 11, pp. 205-230.

Hansen, Lene and Nissenbaum, Helen (2009), *'Digital Disaster, Cyber Security, and the Copenhagen School'*, International Studies Quarterly, Vol. 53, pp. 1155-1175.

Rid, Thomas (2012), *'Cyber War Will Not Take Place'*, The Journal of Strategic Studies, Vol. 35, No. 1, pp. 5-32.

News articles
Burke, Liz (2015). *'World War III will be cyber war that IS could join, John McAfee says'*, news.com.au, 16 December 2015. URL: http://www.news.com.au/technology/online/security/world-war-iii-will-be-cyber-war-that-is-could-win-john-mcafee-says/news-story/45cff1e2e42f062e107183227fec1435 [last accessed on 2 January 2016].

Darrow, Barb (2015). *'Shocker! Amazon remains the top dog in cloud by far, but Microsoft and Google make strides',* Fortune, 19 May 2015. URL: http://fortune.com/2015/05/19/amazon-tops-in-cloud/ [last accessed on 14 January].

Rules and regulation
Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data gathered or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

Websites
Accenture. URL: https://www.accenture.com/dk-en [last accessed on 17 January 2016].

Airbus Defence and Space CyberSecurity. URL: http://www.cybersecurity-airbusds.com [last accessed on 12 January 2016].

Alcatel-Lucent. URL: https://www.alcatel-lucent.com [last accessed on 8 February 2016].

Amazon Web Services, AWS. URL: http://www.aws.amazon.com [last accessed on 11 January 2016].

Atos. URL: http://atos.net/en-us/home.html [last accessed on 8 February 2016].

Center for Strategic and International Studies, CSIS. URL: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events [last accessed on 27 August 2015].

EuroCloud Europe. URL: http://www.eurocloud.org [last accessed on 12 January 2016].

European Digital Rights, EDRi. URL: https://edri.org [last accessed on 27 February 2016].

European Commission: Digital Agenda for Europe. URL: https://ec.europa.eu/digital-agenda/en [last accessed on 14 January 2016].

European Cybercrime Centre, EC3. URL: https://www.europol.europa.eu/ec3/ec3-in-action. [last accessed on 12 January 2016].

European Union Agency for Network and Information Security, ENISA. URL: https://www.enisa.europa.eu [last accessed on 12 January 2016].

IBM Security. URL: http://www-03.ibm.com/security/?lnk=buse [last accessed on 12 January 2016].

Intel Security. URL: http://www.intelsecurity.com [last accessed on 12 January 2016].

International Data Corporation (ICD). URL: https://www.idc.com [last accessed on 17 January 2016].

Microsoft Azure. URL: https://azure.microsoft.com/en-gb/ [last accessed on 8 February 2016].

SAP. URL: http://go.sap.com/index.html [last accessed on 8 February 2016].

Secunet. URL: https://www.secunet.com/en/ [last accessed on 12 January 2016].

SHH Communications Security. URL: http://www.ssh.com [last accessed on 12 January 2016].

Symantec. URL: https://www.symantec.com/index.jsp [last accessed on 12 January 2016].