universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Enacting Digital (In)Security:

The practice of critique in information security research“

verfasst von / submitted by

David Fox

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 906
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Science-Technology-Society
Betreut von / Supervisor:	Mag. Dr.in Nina Klimburg-Witjes, MA

Table of Contents

1. Introduction

On May 12th 2017 hospitals across Britain stopped working. According to reports this involved "shutting down wards, closing emergency rooms and bringing medical treatments to a screeching halt." (CBS News, 2017) The cause of this pandemonium? A computer virus now known as WannaCry. The second most damaging cyberattack ever carried out, the virus caused up to $4 billion estimated in damages across 150 different companies. North Korea has subsequently been blamed by many governments and cybersecurity companies, but have themselves denied responsibility.

On November 8th 2016 Donald Trump was elected president of the United States of America. This election has become one of the most contested in US history - due in part to continued questions and formal investigations into the involvement of various 'illegitimate' actors in his victory. With the campaigns of the Russian state 'troll farm' the Internet Research Agency, the broad network of blogs and bots that campaigned for the president, and the leaking of his opponent's emails by wikileaks – this was, according to one commentator, "the biggest election hack in US history" (Rid, 2016). Similar concerns have been raised about elections in India, Brazil, the UK and Poland amongst others - leading to certain commentators arguing that liberal democratic institutions are under threat due to the weaponisation of digital technologies (Snyder, 2018).

In May 2013 Edward Snowden released 9,000 classified documents detailing global surveillance programs run by the NSA in the US and GCHQ in the UK, amongst others state intelligence agencies, with the support of various telecommunications companies. These revelations led to widespread concerns about the privacy implications of digital technologies and to attempts to make online communication more secure. At the same time due to his unauthorized release of state information Snowden was subject to criminal prosecution from the US government, branded a traitor by sections of the media and remains living in asylum in Russia.

These cursory examples immediately raise some pressing questions about the provision of digital security: What do we mean by and practice as security? What counts as threats? How do we know so? Who should be secured? With what means? And: Who decides on the answers to these questions? This thesis will essentially be an exploration of how one particular group answers these questions: information security researchers. It will look at how security is understood, made meaningful and practised within the everyday research of digital security.

Attempts to keep information secure and private are as ancient as interhuman communication itself (Dlamini, Eloff & Eloff, 1991). From the construction of private rooms in Palaeolithic times, to the codes constructed in Ancient Egypt, there are abundant examples of historical information security practices. In the last 60 years, though, these practices have found a new focal point: digital technologies. As the examples above indicate, the field of digital security is now a broad multifaceted one, with various digital technologies entwined with ever more parts of our lives and their institutions. As Bruce Schneier (2017), a prominent writer on information security, puts it:

> The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in. This is the future, and what we're calling the Internet of Things. [...] Once computers start affecting the world in a direct and physical manner, there are real risks to life and property. There is a fundamental difference between crashing your computer and losing your spreadsheet data, and crashing your pacemaker and losing your life.

It is within this environment that information security researchers are situated. These actors research various ways to ensure digital information's confidentiality (that communication remains private), integrity (that information is not changed by unauthorized parties) and accessibility (that authorized actors can access the information). They analyse different technologies, search for their vulnerabilities, explore new security techniques, analyse the behaviour of attackers, advise groups on how to improve their security and more besides. A guiding assumption of this thesis is that through practising these different forms of research, a

distinct form of security also gets performed. The general question I am interested in is, given the breadth of digital security, its continued rapid expansion, and the heterogeneous and contradictory interests involved, how do the researchers choose areas to focus on? What seems, to them, valuable enough to protect and why? What institutional mechanisms interact with this decision? And, returning to the examples and questions above, what sort of security emerges with these choices?

One source of inspiration for this concern is literature from critical security studies (CSS). The central research project of this field has been to explore the various ways that things become defined as security threats and the effects of such a construction. Understandings of this process have generally moved from a straightforward narrative of powerful political elites 'securitizing' through discursive pronouncements, to a more differentiated image of security being varyingly negotiated by different groups across a broad 'field' of security. These groups include "professions of urban policing, criminal policing, anti-terrorist policing, customs, immigration control, intelligence, counter-espionage, *information technologies,* long-distance systems of surveillance and detection of human activities, maintenance of order, re-establishment of order, pacification, protection, urban combat, and psychological action." (Bigo, 2008, p. 15, emphasis added). The subsequent empirical programme has been to look at these different professional groups, and "to differentiate clearly between various parties' standpoints on how to prioritize threats*"* (REF) and how to prioritise objects to be secured, security methods to be employed, actors to be made responsible etc. It is intended for this thesis to be a contribution to this project, giving a detailed empirical account of the (in)security practices within one site of contemporary security provision: information security research.

Even within this differentiated perspective, though, information security research is still quite an idiosyncratic security institution. Broadly that is because it does not operate strictly within the traditional boundaries of state security. While the discipline's boundaries do indeed overlap with certain national security agencies (a glance at the funding of central conferences proves as much), they also do so to a great extent with various other groups such as computer scientists, consultancy firms, tech multinationals, security companies, 'subversive' hacker subcultures etc. Furthermore, information security researchers are an odd security group to study in relation to literature from CSS because they are *researchers*: they work in academic institutions, publish papers, present at conferences, search for funding for

their research. If we think about CSS's usual research focus mentioned above - the prioritization of security concerns by different groups - within this context, my research problem becomes a different, more mundane one: why do researchers focus on different areas within the academic field of information security?

These processes related to the academic life world are quite far removed from the usual empirical cases of CSS and have more so been the focus of Science & Technology Studies (STS). From the foundational laboratory studies, to accounts of various epistemic cultures across the sciences and the more recent focus on valuation enactments in research, STS scholars have continually provided insights into the various practices constitutive of knowledge production, To explore this research problem, I will draw from the theoretical tool kit of valuation studies, looking at research as a site of various valuation practices, and research focuses as both in themselves enactments of value and as partially emergent from other personal and institutional value practices. I also hope that the thesis will be a contribution to valuation studies, by further extending the field's inductive treatment of Luc Boltanski's work to more of his theoretical framework. Three specific concepts of his will be used in this inductive manner to elucidate the valuation practices found in the research centre: *justifications* (how actors express the worth of their own activities) *critiques* (how actors negatively assess various activities, actors, institutions etc.) and tests (institutionally embedded determinants of value). Luc Boltanski's theoretical framework also offers itself as an appropriate source for this thesis, due primarily to his (somewhat ambivalent) position between the critical sociology of Pierre Bourdieu and the pragmatic sociology of Bruno Latour, important inspirations for CSS and STS respectively.

With this I centrally want to treat a research problem presented by critical security studies with a sensibility derived from Science and Technology Studies. I further, though, want to draw out certain implications of this move. On the one hand, I want to explore the insights that a theoretical approach derived from STS can bring into discussions in CSS - highlighting, for example, the contingencies and complexities that are an important, and sometimes overlooked, part of the provision of security. I am also though interested in the difficulties in bringing these two approaches together and the frictions that arise when doing so. Important here, particularly, is the notion of critique. A central finding of this thesis will be that the work of information security scholars is a specific critical activity - one that has a relatively close position vis-a-vis its object of critique. Both within STS and CSS the notion

of critique has been discussed in recent years, while it has also been a central focus for both Boltanski and Bruno Latour, both important inspirations for valuation studies, and pragmatic sociology more generally. While these ideas do bear similarities, used by both to differentiate themselves from Pierre Bourdieu, it is also one of the most divergent parts of their theoretical repertoires, with Latour having a broadly negative assessment of a large range of critical activities and Boltanski a broadly positive perspective. This thesis will contribute to these discussions with an agnostic analysis of the critical activities of information security researchers, a rather idiosyncratic critical group. It will use this as an opportunity to engage in questions about how critique is differently understood and practised in STS, CSS and information security research. The tensions between these different practices will be acknowledged, but attention will also be paid to their resonances and the possibilities for them being fruitfully brought together.

The thesis will proceed in the following way. The first chapter will sketch out certain broad empirical trends, important to situate the later chapters. A short history of both information security in general and of the academic discipline will be provided, followed by a more detailed look at SBA Research and the different types of work carried out there. Following this the current state of the art of literature relating to this case will be discussed. This will contain two central parts. Firstly, the different approaches to the study of security will be outlined, focusing particularly on Critical Security Studies and contributions to this field of study from Science and Technology Studies. Secondly, literature focusing on cybersecurity will be outlined. It will be found that these studies have generally not explored the world of academic information security, and that the theoretical tool kit of Boltanski and Valuation Studies would make a useful contribution to this literature. This theoretical framework will then be developed. Three concepts central to Boltanski's framework and that will also be used in this thesis - justifications, tests and critiques - will be outlined. The central theoretical contribution of this thesis will be to treat these concepts with the inductive sensibility found within valuation studies, further extending this approach's use of Boltanski. The fifth chapter will outline the research questions that have guided this project's empirical research. The sixth chapter will outline the methodology that these questions were answered with - semi structured interviews analysed with grounded theory - while pointing to reflexive tensions that were important for my engagement with this case. The empirical findings will then be presented, arranged according to the central three processes that the thesis is

concerned with - critiques, justifications and tests. More precisely, the critical activities of the researchers will first be considered, both occurring within and outside of SBA Research, using this comparison to highlight the specificity of information security's disciplinary critical activity. The justifications that the researcher's offer for their work will then be outlined, with three central sets found, focusing respectively on protecting users, engendering trust in digital technologies and fulfilling the researchers own demands. The institutional tests that the researchers work is subject to - getting funding and being accepted to conferences - will then be presented. The final chapter of the thesis will relate these findings to the literature presented earlier from STS, CSS and valuation studies, finishing with some proposals for future research.

2. Empirical case

This section will give an outline of the empirical case at the centre of this thesis – information security (research) and SBA Research. First, a short history of the various practices used to secure information will be provided, looking at how this has developed very generally, particularly since the advent of computers. Second, the academic discipline of information security will be outlined, pointing towards its historical development, its current state and certain key concepts within it. Finally, SBA Research itself will be described and the different types of research conducted there outlined.

2.1 Information security

The history of information security is formidably long and complex, with all groups of humans engaging in certain practices to keep communication secret (MacMillam, 2011), thus a comprehensive review of these practices would be more than a lifetime's work and will not be attempted here. Rather I will provide a very simple narrative of certain obvious overarching developments, to just point towards the historically situated nature of the field being researched.

According to Dlamini, Eloff & Eloff (2009, p. 190) "information security is as old as information itself". As long as humans have tried to communicate secretly some form of protection mechanisms have been put in place: from walls separating rooms, to soldiers guarding messages. The practice of cryptography, or the technique of writing messages in code so that they can be kept secret, is said to have begun in ancient Egypt, where certain hieroglyphic symbols were substituted for unusual ones that obscured the meaning of the inscription (McDonald, n.d.). From this to Thomas Jefferson's wheel cipher in the 1700s, and the various attempts to communicate securely and privately during WWI, history is abundant in examples of some form of securing information (cf. de Leeuw & Bergstra, 2007). A narrower definition of information security, though, provides a shorter history. In the popular textbook *Principles of Information Security,* Whitman & Matford (2017) trace the history of information security to the invention of computers, and their use within WWII. This computer security was focused on securing the "physical location of the computer from

outside threats" (p.4), but also breaking codes of intercepted communications from the technology. Here already the dual use of computers within security can be seen - the need to defend this important asset, but also their usefulness in achieving certain security ends.

This double sided use continued during the cold war, with the notable development of the ARPANET by the US Department of Defence's Defence Advanced Research Projects Agency (DARPA), which would later develop into what is now referred to as the internet (Murphy, 2019). With this also emerged one familiar aspect of contemporary information security - computer viruses. A programme that is often cited as the first computer virus is called CREEPER - a benign computer worm that displayed the message "I'm the creeper: catch me if you can" on infected computers. Another early example is the Morris worm in 1988, a self-replicating programme that was intended to simply test the security of the internet, but ended up being more damaging than intended, significantly impacting on the performance of affected machines and the functionality of the internet in general. In the years since the public release of the internet, the number and scale of attacks has risen sharply. It is estimated, for instance, that cyber attacks caused some $45billion in financial losses in 2018 (Online Trust Alliance, 2019). The most financially damaging cyber attack of all time is NotPetya - a ransomware programme that attacked a number of different countries, particularly Ukraine, with estimated damages of circa $10billion. Other notable attacks include Stuxnet - a cyber attack on Iran's nuclear programme by the USA and Israel, or the WannaCry virus attributed to North Korea. Simultaneously there has been the growing prominence of 'hacktivists' such as Anonymous, Wikileaks and Edward Snowden in recent years - non-state actors engaging in attaining and publishing (cyber) information for various political ends.

2.2 The academic discipline of information security

This section will focus on the development of the academic discipline of information security. No thorough intellectual history of the discipline itself has been conducted at this time and it would again be a project of far greater scope than this thesis to carry out such an endeavour. The history presented will thus be necessarily cursory, with several specific histories taking the place of a more linear and coherent narrative.

From what was outlined above certain important elements are already clear - the fact

that this research has not taken place only within the academy but within the institutions of various stakeholders - in military institutions, for instance, private companies, and international research centres. Early research into information security, like with computer science in general, was not very institutionalised and emerged from a variety of different institutions and academic fields such as mathematics, information science and electronics, (Cooke, 1992). The beginnings of more disciplinary academic research can be partially traced by looking at the conferences held in the field. The Institute of Electrical and Electronics Engineers (IEEE), for instance, has held its Security & Privacy Symposium since 1980, making it the longest running conference in the field, while remaining one of the most prestigious. Other notable early conferences include USENIX which began in 1989, while the hacker conference Defcon started in 1992

At the 2019 Security and Privacy symposium a retrospective presentation and discussion was held to celebrate the conference's 40th birthday. Mathias Payer (IEEE Symposium on Security and Privacy, 2019a) first presented a general overview of the 'wild ride through time', where he presented the results of a bibliometric analysis of the development of the conference. A particularly useful resource in this presentation is the outline provided of the main topics that were common within each of the four decades of the conference. These are:

> **The 1980s** he referred to as a time of 'Security utopia' - where the dominant feeling amongst researchers was that 'we can do it!' and that digital systems could be fully secured. Here dominant topics and approaches were formal mathematical methods, models that allowed users with different clearances to use a machine in different ways (multilevel security), and intrusion detection.
>
> **The 1990s** he argued were dominated by the introduction of 'The internet!' and a subsequent focus on networked computing. Research was at this time on protocols for defining secure online communication, security based on computer programming languages (now, according to Payer, considered as ineffective) and software testing.
>
> **The 2000s** was a period of fast digitalization that amounted to people beginning 'living in cloud city'. Virtual machine security (focused on virtual emulations of

computers), isolation of different systems, privacy and the relationship between open source software and security were topics studied at this time.

The 2010s was when blockchain, machine learning, analysis and study of data sets, browser exploitation, measurement studies were prominent focuses of research.

Afterwards a panel discussion was held with a more reflective look at the changes in the conference and the discipline as a whole (IEEE Symposium on Security and Privacy, 2019b). One theme that emerged here was the increase in the size of the field - the exponential growth in numbers of papers submitted and the subsequent difficulties in keeping track of developments in the field. Related to this was the growth in interest in the field from those outside of the community ´according to Deborah Frincke "I think of the last decade as when privacy and security became real for the world outside of professionals" (19:07). Explaining the growing complexity of the field, moderator Giovanni Vigna pointed to the increasing complexity of the technological systems. While most of the conversation was generally uncontroversial, a small disagreement arose when discussing the *priorities that the field should take.* Here Vigna argued that "as we make technology more secure it becomes more of a people problem than a technology problem." Voicing her 'complete disagreement' Dorothy Denning said that "technology is moving faster than we can understand it… to think that we can solve the technology piece is just crazy" (49:30).

Another important way to get a sense of the discipline of information security and the historical changes therein is through the central concept of the 'CIA triad' - where research aims to protect the confidentiality, integrity and accessibility of information - and how different parts of this triad have been prominent at different periods. Confidentiality refers to keeping data private: "defining and enforcing appropriate access levels for information." Integrity is focused on making sure that the information is not modified or deleted by unauthorized parties. Availability is about making sure that data remains accessible to authorized parties - i.e. to protect against ransomware attacks which shut down a computer or digital system unless a financial payment is made. Bruce Shneier (2016) argues that computer security has traditionally focused mostly on issues around confidentiality, but that threats to the integrity and accessibility of information are becoming increasingly important. He also argues that these threats are "much more visceral and much more devastating", supporting

this with reference to the potential implications of attacks on driverless cars: “Someone who can feed the cars false information can potentially cause them to crash into each other or nearby walls. Someone could also disable your car so it can't start. Or worse, disable the entire system so that no one's car can start.”

Another helpful resource in understanding the current shape of the discipline is Dunn Cavelty and Egloff’s (2019) bibliometric analysis of academic publications about cybersecurity in the Web of Science and Scopus Databases. One point here is again the growth in interest in the topic: “from 2012 to 2014, the quantity of scientific output on ‘cybersecurity’ almost doubled.” (p. 40) They further point out some specific characteristics of this output - that most publications come from computer science (WoS: 72 percent / Scopus: 61 percent), with the second discipline being engineering (WoS: 36 percent / Scopus: 40 percent), and that all of the top ten entries in both sources “focus on smart grids and/or SCADA (Supervisory Control and Data Acquisition) systems, a category of software used in many industrial processes to control equipment and conditions.” (ibid) They finally sum up the focus of this literature as: “The main aim of research is to develop better cyber incident prevention, protection, and detection capabilities on the one hand, and more ‘resilient’ systems and infrastructures, signifying timely recovery of functionality if under duress due to an attack, on the other.” (ibid) They relate these findings to their overall research interest - the variable role of the state within cybersecurity literature - arguing that this technical literature is generally not interested in the state. While this research is a useful indication of the broad scope of the field, it also quickly moves on to other areas of research, largely social scientific, and fails to give an in-depth account of the complexities and political implications of the technical field of research. A central claim of this thesis is that this area of research is itself a site of rich data for social scientific data, and that delving into the complexities of this research is helpful in exploring developments in the contemporary provision of security.

2.3 SBA Research

This thesis will further focus on one particular site of information security research: SBA Research, an information security research centre in Vienna, Austria. With over 100 employees, SBA is the largest research institution in Austria focused exclusively on IT security. It is also the longest running such centre in Austria, having been founded in 2006 in

a partnership between TU Wien, Graz University of Technology, and the University of Vienna.

The centre has a number of wide ranging focuses. Research conducted here is said to be both applied and basic, although the latter is still understood as leading to future applications. It is claimed that a general the aim of this research is that "it protects IT infrastructure and data against damages done by persons or events." (SBA Research, n.d.a). Research in SBA is organised around four areas, which "allow a comprehensive consideration of information security" (SBA Research n.d.b, p. 3):

1. Networked systems security: "approaches to the main security challenges of networked systems"
2. Software systems security: "comprehensive, lasting solutions to automatically and transparently harden software"
3. Privacy and Secure Societies: "privacy-protecting mechanisms, the analysis of deployed systems and how the privacy of individuals can be enhanced at large"
4. Applied Discrete Mathematics for Information Security: "the future of cryptography and combinatorial security testing"

A sense of the general research carried out at the centre can further be seen with reference to some of the groups and projects currently active therein:

- The Decentralized Systems Group (n.d.), for instance, focuses on the potential benefits and threat scenarios of blockchain and distributed ledger technologies. Current projects focus on "the secure execution of smart contracts, alternative applications for Bitcoin and cryptocurrencies, cross-chain interoperability and blockchain consensus mechanisms." Through this the group hopes to offer a "glance beyond the hype", to a place where "the core question is not whether "blockchain" is applicable but which of the existing approaches is most suitable."
- Another cluster of research is centred around the Mathematics for Testing, Reliability and Information Security (MaTRIS) Research Group. This group facilitates "the connection between discrete mathematics, computer science in general and, in particular, the interplay with information security." The group argues that their

research has contributed to the "development of real world applications" and "theoretical approaches and methodologies." There are two main strands of research within this group: Combinatorial Security Testing - which allows for an automated detection of security vulnerabilities and Covering Arrays, Algorithms & Optimization (CALGO) - which develops mathematical formulae to indicate a set of configurations of a software that is sufficient to discover its level of security.

- FeatureCloud is one recently announced project that SBA Research will contribute to. This project is focused on the application of 'cloud infrastructure' to the healthcare sector. The project envisions "a future in which doctors can easily and safely store, access and manage primary medical patient data without risking a privacy breach", where patients have "full control" over their medical records and researchers "have global access to truly anonymous medical and biomedical data" (FeatureCloud, n.d.). SBA Research have responsibility for security and privacy related topics within the project.

An interesting point to note is that my organisation of the researchers does not accord with these formal delineations provided on the website. I have primarily arranged the researchers according to their specific focus points – internet of things, usable security, blockchain - descriptions which were given to be by my gatekeeper, who has an administrative role within the centre. The researchers themselves also aligned rather with these categories than any of the specific four areas outlined on the SBA website. Indeed these formal categorisations were not once referenced within the interviews. While the centre is focused on research, it also engages in a number of other activities and in line with this the centre positions itself as "A Bridge Between Science and Industry". Specifically they make their scientific results accessible to "IT Decision Makers" (SBA Research n.d.b, p.8), by developing partnerships with "industrial and public partners" (ibid) and through educating future experts. Its website also indicates that they are also committed to social responsible research - encouraging a broad awareness of security issues through talks, workshops and other outreach efforts (SBA Research, n.d.b). They also support new entrepreneurs with their 'accelerator programme', providing funding and guidance to young people developing innovative security products. These brief overviews hopefully point to certain ways that SBA is a distinct information security research centre, situated in a number of different historical and socio-economic

processes, important to briefly note, but largely beyond the scope of this thesis.

3. State of the art

In this chapter a range of scholarly discussions relevant to this thesis will be outlined. Most broadly, certain strands of research on security will be considered, particularly work within the overlap between Science & Technology Studies (STS) and Critical Security Studies (CSS). Within this, social studies on cybersecurity are particularly important for this thesis. A first set of arguments from this section relate to the interactions between STS and CSS: that there are often unacknowledged theoretical tensions between the two fields, and that CSS borrows from a limited range of concepts from STS. Another central claim in this chapter is that research informed by an STS-consonant theoretical framework has brought out important lessons about the provision of contemporary security and would be a useful contribution to studies of cybersecurity.

3.1 Security Studies

This section will present a broad overview of research within the discipline security studies and, particularly, the various strands of 'critical' literature that have emerged in the last 30 years, crucial for situating arguments that will be subsequently developed in this thesis. Following this the different contributions of STS to the study of security will be outlined. Through this engagement I want to underline that while STS concepts have been useful and influential within the (critical) study of security, that the tensions that exist between these approaches and those traditionally drawn upon by CSS scholars have largely been overlooked. Furthermore, CSS scholars have largely drawn from a limited set of STS theoretical contributions, and exploring other approaches might provide alternative paths for these disciplines to productively interact with each other.

3.1.1 Orthodox approaches to security

Security and defence have, of course, been topics of study from time immemorial, with ancient contributions from Thucydides in Greece, Sun Tzu in China and Augustine in Rome. The institutionalised field of security studies, though, only developed following the second world war (Buzan & Hansen, 2009, p. 8), developing as a subdiscipline of international

relations (IR), with its particular focus on the use of force in international affairs, and, more precisely, "state use of military force" (ibid, p. 16). For these orthodox security studies scholars, particular issues attain a 'security' character - and are thus of concern to the subdiscipline - because they are intrinsically threatening to states, and thus provoke a response based on military force. As such, this leads to nation-states being positioned as the primary *referent object* of security - that is, they are the thing that must be secured by the relevant state (Kerr, 2003). Centred around the political climate of the cold war, the rivalry between the US and Russia, and the presence of nuclear weapons, much early security studies scholarship was ideologically committed to US hegemony and understood the Soviet Union in particular as a potentially existential threat. Central questions within this era were around the possibility of nuclear warfare, the ways for this to be deterred (while still achieving US strategic victories), and explanations of the apparently stable Cold War world order (Buzan & Hansen, 2009, p. 66-91).

Epistemologically, security studies adopted a thoroughly positivist approach during most of the Cold War era, and realist perspectives that are prevalent in IR have also been prominent here (WoWohlforth2009). Contemporary realist theories' fundamental assumption is that the international order is anarchic - there is no overarching authority to enforce rules or provide order. As such, states, the fundamental units of analysis, are understood to be placed into competition with each other for power and survival, and to be motivated primarily by a calculating self interest - which amounts to an application of the rational actor theory, common within economics, to international affairs. Games theory is a frequent form of security theorizing based on these assumptions. The notion of games comes from Von Neumann's influential work within economics, where games are said to be situations with multiple rational actors where the utility of one actor's actions is based on the actions of the others (O'Neill, 1990). The focus of analysis is to determine the equilibrium of various games within different situations - the likely or mathematically necessary outcome of the games. Within security studies these were often applied to the issues of nuclear warfare and the conditions that might provide for its outbreak or continued deterrence, as well as the possibilities for cooperation within an anarchic system .

3.1.2 Critical security studies

This orthodox school of security studies has, though, been criticised by a diverse range of scholars since the 1980s, and particularly since the end of the Cold War. Early critiques focused on normative issues, with many arguing that the security studies tradition was overly attached to US strategic aims, as well as policies of nuclear armament. They moreover claimed that the narrow focus of orthodox security studies left many important areas unexplored. Peace scholars, for instance, bemoaned the focus on warfare and state security, and the way that peace was understood 'negatively' - as simply the absence of warfare. They instead argued for the study of the 'positive' elements that would be needed to bring about lasting peace - reconciliation procedures, for instance, or the construction of more just social systems (Galtung, 1969). Feminist critics at the same time highlighted the gendered dynamics of security, looking at, for example, the fact that women were found to have attitudes that had more sceptical views on warfare and military practices than men, while also pointing to the exclusion of women within security scholarship (Boulding, 1981). Important also is the 'Aberystwyth school', early proponents of 'critical security studies', who contributed a perspective informed by Marxist critical theory to debates about international security. They opposed the state-centric nature of orthodox accounts as this, they argued, supported the international status quo. They argued for a 'broadening and deepening' of security studies (Krause & Williams, 1996), where actors other than the state could be positioned as the referent object, while non-military threats, including economic and environmental, should be included within analyses. They also held a positive view of the process of defining something as a security threat, seeing this as a necessary step in an emancipatory political project.

This specific point, about the different ways that security threats come to be defined and employed, is something that poststructuralist and linguistic scholars have subsequently expanded upon. The 'Copenhagen School' of security studies offer one particularly important elaboration of this theme, best captured through the famous *securitization theory* (Wæver, 1993). Influenced by the performative linguistic theory of J.L. Austin, this approach conceptualises the designation of something as a security concern as a particular type of 'speech act': utterances that do something through the very act of being spoken. Everyday examples of speech acts include statements like 'I promise' or 'I am complaining about X': acts that are constituted by the pronouncement of a particular statement alone. With

securitization this means that by discursively naming something a security issue, this moves certain issues out of normal politics and, according to central theorists, into less democratically accountable spaces (McDonald, 2008). Thus elite political actors are understood to be those with sufficient power to securitize an issue. 'Security' is furthermore seen here in a more negative light than with the Aberystwyth scholars, with theorists from Copenhagen largely arguing against processes of securitization. Elaborations on this initial formulation have emphasised the need to consider the role of audiences in legitimating speech acts, the power of securitizing actors not considered in the original formulation (Balzacq, Leonard & Ruzicka, 2016), while others have looked at how this focus on speech can further silence marginal actors within security politics (Hansen, 2000).

Another strand of thought within critical security studies important for this thesis is the so-called 'Paris school', which in general emphasises the *everyday practice of security* (Bigo & McCluskey, 2018). This group of scholars emerged from political sociology, with studies centred around the sociology of policing and migration in Europe who introduced an "agenda focusing on security professionals, the governmental rationality of security, and the political structuring effects of security technology and knowledge" (C.A.S.E. Collective, 2006, p. 449). A central finding here was the emergence of a field of security within the EU, and with it the increasingly blurred boundary between internal and external security. This notion of field is drawn from Bourdieu and emphasises the diffuse but interconnected nature of contemporary security practices as well as the dynamics of power between the heterogeneous groups involved. These are said to include "professions of urban policing, criminal policing, anti-terrorist policing, customs, immigration control, intelligence, counter-espionage, information technologies, long-distance systems of surveillance and detection of human activities, maintenance of order, re-establishment of order, pacification, protection, urban combat, and psychological action." (Bigo, 2008, p. 7) In line with this a central aim of research is to explore how security is *understood and practised* differently within distinct social worlds - exploring how:

> *"the "field" is determined by the struggles between police, intermediaries and military agencies about the boundaries and definition of the term "security", and around the prioritization of the different threats, as well as the definition of what is not a threat but only a risk or even an opportunity."* (ibid, p. 24)

Thus the abstract and linear model of security provided by the Copenhagen School is replaced with a more supple empirical programme, that draws out the complexities of contemporary security practices. This is one of the main projects that this thesis is aimed at contributing to - unpacking the way that security comes to be understood and practised within the specific security world of information security research.

Quite a large number of empirical studies have been conducted within this general project, and Bigo's (2014) anthropology of three different 'universes' of European border control - a navy boat, border stations and a data-analytics center - is an indicative example. Here he argues that the control of borders is informed by practitioners' 'practical sense' - an everyday understanding of borders, control and (in)security - developed within these distinct social worlds. Important to underline here is the specific understanding of *practices*, derived from Bourdieu and his notion of habitus, that informs this analysis: "[t]he habitus is the origin of the practices that reproduce or change the existing structures of the field. These practices again shape the experiences of actors, form their habitus, and stabilize power structures in the field." (Bueger & Gadinger, 2015, p. 455) Practices here are embodiments of a particular social structure and help to stabilize specific social worlds, rather than the messy generative understanding of practices more common within STS. Also relevant to this thesis is that, while the various sites considered relevant to security theorists is significantly broadened here, they remain somewhat narrowly defined. This, Emma McCluskey (2017) argues, is reflective of much of the work done within this 'Parisian' tradition, which "though enlarging the meaning of 'security', nonetheless tended to operate within a pre-defined space and a somewhat preconceived notion of what a 'security' site of research should look like. Certainly, 'doing' ethnography appears to be conducting research on traditionally 'powerful actors' such as within security agencies [...], with military personnel [...] or in war or conflict situations" (p. 1).

An important question for this thesis is what it might mean to explore a security site as idiosyncratic as information security research. Furthermore, how might the use methods derived from a school of thought in open conflict with Bourdiean critical sociology - the French pragmatic sociology of Bruno Latour and Luc Boltanski - challenge the assumptions that Parisian studies are reliant upon? The next sections will begin to answer these questions, exploring how STS ideas have been utilised within CSS, as well as how STS scholars

themselves have addressed security issues in their work, pointing to both convergences and divergences in these approaches.

3.1.3 Science & technology in security studies

In recent years concepts and sensibilities from STS have been increasingly utilised by scholars within the various strands of both IR and CSS, but mostly from scholars associated with the 'Paris' school of security studies. This section will look at some different aspects of these uses, underlining the contributions that these approaches offer to the study of security.

While there are a number of different STS concepts that have been introduced into critical security studies, most commonly invoked is Actor-Network Theory (ANT). Some contributions situate this usage of Actor Network Theory within a broader turn to materiality within international affairs. and particularly the increasing entanglement of security practices and technological apparatuses. In this line of reasoning STS opens up new sites to be explored by security scholars. Mark Salter's collection of essays, *Making Things International* (2015), is a prominent example of this kind of work. Essays here look at various different non-human actors - including containers, corpses and cocaine (to take the essays beginning with c) - and explore their relation to international politics. What this amounts to is a widened understanding of where security politics can be and thus a broadened terrain within which research can be conducted. As Debbie Lisle (2014, p. 67) puts it, "the 'materialist turn' has energized the scholarly landscape by allowing us to recognize the political in a radically expanded landscape of sites, scales and temporalities."

While this focus on objects within the study of international security is indeed novel, another way to frame this change in relation to practices. Repeating from the previous section, this is related to a different understanding of practices from the Bourdieu inspired Parisian critical security studies. Bueger and Gadinger (2015) argue that 'the pragmatist tradition' which draws from Latour and ANT amongst others *"*aligns the concept of practice closer to action and, as a result, it loses its structural connotations. [...] Thinking of practice in terms of change is at the core of the pragmatist tradition and reflects the aim of reconsidering "agency" in a more substantial manner.*"* (p. 455) Replacing a concern with domination and hierarchical orderings of social worlds, pragmatist practice theorists instead focus on issues around "uncertainty, creativity and situated agency" (ibid). As such ANT or STS informed approaches often present a messier and more complex image of the provision of security.

Davidshofer, Jeandesboz and Ragazz (2016), for example, offer a study of the 'technological imperative', but here the analysis, drawing explicitly from Bourdieu, focuses on how historically embedded 'patrimonies' determine the practice of this imperative. Here the analysis remains heavily 'sociological' - emphasising how social patterns of behaviour or pre-established values determine the use of technology, rather than the emergent complexities of novel sociotechnical configurations.

One particularly noteworthy use of ANT ideas is Jef Huysman's concept of 'little security nothings' (2011). In this paper he argues that the framework helps to disrupt the concept of action within security studies, and that ANT's distributed understanding of agency is useful to understand the diffuse practices that characterise contemporary security. As he says: "Securitising develops through a wide variety of mediators that connect data, people, sites, and times but in connecting also change the material they are connecting" (p. 7), arguing against the emphasis placed on isolated elite actors within the Copenhagen school's securitization theory. He thus suggests that ANT's notion of agency helps to both recast mundane and distributed actors as relevant for the politics and study of security, and also reconfigure our understanding of these actors. Marieke de Goede (2018) has made a similar, if more empirically applied, argument to this. She looks at how this notion of agency can be helpful in politicizing tech companies' roles in distributing information in a way that is apparently banal, but ultimately renders people as subjects of a security apparatus. Borrowing Latour's notion of chain of translation, de Goede conceptualises "the path of the suspicious transaction as a chain of translation, whereby commercial transactions are collected, stored, transferred, and analysed in order to arrive at security facts" (p. 27), thus highlighting the security roles of these translations and the actors carrying them out .

Ideas related to STS and ANT have been employed recently on quite a distinct topic: reassessing the notion of critique within critical security studies. This issue was discussed most prominently within a special issue of Security Dialogue on 'Doing and mediating critique', that commemorated the prestigious journal's 40th anniversary. Austin, Bellanova and Kaufmann's (2019) introductory essay was most explicit in the theoretical connection to STS. The authors here expressed concern with the critical activity currently conducted with CSS - that "[c]ritique frequently has normative ambitions, but few ways to actualize them" (p. 4). They argue that this can be counteracted with a praxeological understanding of critique, where critique should be seen as practised in relation to, using Donna Haraway's

terminology, 'companions': "that the ideas produced by the critical scholar and inscribed in her text are produced at least partially externally to the academic field: by persons, material things, and other practices or networks that mediate those ideas across time and space." (p. 6) The authors explicitly invoke Bruno Latour and ANT as a reference point for the diagnosis of the contemporary failure of critique, as well as for the ways that this can be reoriented. Leese, Lidén & Nikolova (2019) provide an empirical example of what such a practise of critique might look like. They discuss their work with ethics procedures that EU funded security research is subject to, and re-conceptualise this as a site where critical ideas can be implemented. They remain ambivalent about the possibilities of this being productive though, citing problems with political ambitions, economic interests and technological rationales amongst security professionals. They argue that with such a practice comes the risk of "legitimizing problematic research and development activities through one's very participation." (p. 65)

A central argument I would like to make here is that, while approaches from STS have proven to be productive within the critical study of security, this project should not be limited to simply exporting ANT into CSS. Rather, first of all, the ramifications of this move must be taken into account, and the tensions between the different theoretical frameworks explored. As Aradau and Huysmans put it: "Although these authors have inspired much of the recent critical work on 'security practices' in international relations [...], the controversy between Bourdieu's sociology of practice and science and technology studies has received much less attention" (2018, p. 7). Furthermore STS have a number of approaches other than STS, that are currently underexplored within critical security studies, that might have different relations with the critical tradition that CSS draws from. The next section will attempt to further open up these discussions, through an examination of the distinct approaches taken to security by scholars within the STS community.

3.1.4 STS on security

This section will explore approaches to security that have come from Science & Technology Studies scholars. It will look particularly at the different theoretical traditions that have informed this work – pointing to how CSS scholars borrow from a specific strand of STS thought - while also looking at how research institutions have been explored as sites relevant to the study of security. Lastly, the specific arguments around engagement given by certain

STS scholars focused on security will be outlined and discussed in relation to the notion of critical companionship, above.

While a sustained focus on security has mostly emerged in STS in the last two decades, prior to this certain security relevant devices (particularly, weapons) have been intermittently used as examples to give empirical weight to some of STS's more theoretical propositions. Bruno Latour (1999), for instance, has famously used a shotgun as an elaboration of his ideas around distributed and collective agency. Here Latour's long standing arguments against rigid subject-object distinctions and strict delineations of agency are grounded in a rather dramatic example:

> *You are different with a gun in your hand; the gun is different with you holding it. You are another subject because you hold the gun; the gun is another object because it has entered into a relationship with you. [...] If we study the gun and the citizen [together] [...] we realize that neither subject nor object [...} is fixed.* (179–80)

A similar argument is offered by Woolgar and Grint (1992) in their debate with social informatician Rob Kling. They again criticise any attempts by theorists to attribute inherent capacities to technologies, again in this case guns. They call for a purely discursive analysis, where the various positions taken by actors in the debate are evaluated, looking how these different discourses attribute agency and the effects of these various attributions. These early applications, though, were quite sporadic and did not amount to a consistent programme of research.

Lucy Suchman is one theorist who, drawing from a related ethnomethodological tradition, has given sustained attention to security issues. In this work she extends her long standing interest in the new forms of agencies that emerge as an effect of human-machine interaction to security practices, looking particularly at the way that responsibility can be rethought as a result of these conceptualisations. In one essay Suchman and Weber (2015) problematise the discourses around making autonomous weapons systems responsible through the presence of a human 'in the loop', arguing that this relies on an untenable static conception of human subjectivity. Her point is that the technosocial apparatus that this human is situated within changes their decision making processes and "that the 'loop' in which humans and machines are conjoined in contemporary weapon systems, whether the humans

are figured as 'in' or 'on' that loop, diminishes the possibility of judgements not to kill" (p.102). This argument uses a similar logic found in Latour's piece, but draws out concrete political implications from this embedded view of human agency.

Most other literature from STS scholars on security issues is quite different from this work, with one major difference being the theoretical approaches which are generally more in line with Sheila Jasanoff's ideas, than with ethnomethodology or ANT. Witjes and Olbrich (2017) for instance analyse the development of satellites using a lens of co-production, allowing the authors a wider perspective that takes into account institutional transformations. They explore the relationship between changing actor constellations and notions of transparency and power, questioning the uncritically supportive narratives around the use of satellites and the transparency they will bring. Instead the authors argue that this transparency should be viewed as 'fragile' - which emphasises "its contingent emergence, limited scope and, in particular, its context dependence." (p. 532) Clark A. Miller (2015) has also described changes in understandings and practices of security using another of Jasanoff's concepts, in this instance sociotechnical imaginaries. He points to the 'globalised nature' of contemporary understandings of threats and insecurity - pointing to climate change and pandemics - and looking at the specific institutional changes that these have brought about. It is important to note here how Jasanoff's particular theoretical framing allows the researchers insights into the connection between security and technoscience on a different scale than with Suchmann or Latour, as well as the diversity of approaches to security that STS has provided.

One important strand of research within this has looked more closely at the entanglements between certain areas of scientific practices and security concerns, positioning scientific research sites and institutions as important within contemporary security concerns. Certain studies here look at the development of technologies used for security within research institutions. Möllers (2017), for instance, has looked at how researchers dealt with conflicting pressures from the state, the wider public and academia in a project focused on a 'smart' surveillance system. She situates her work within debates around neoliberal science and argues that these debates often overlook the personal conflicts that individual scientists go through, often painting them as either entirely subservient or resistant to external demands. She highlights the various forms these pressures can take, and the ways that scientists deal with them. When, for instance, dealing with the difficulties in labelling dangerous behaviour, which was also seen as technically uninteresting, the researchers creatively adopted a model

of deviancy within groups of seagulls to the system - thereby satisfying the demands of the government while also circumventing the ethical and technical difficulties of defining such behaviour. The researchers in general were motivated more by academic concerns than by those of the governments and funding agencies, but then 'tailored' their results to these groups - a tailoring that consisted of a continuous negotiation that also impacted on the contents of the research. Important to note here is that though Möllers's piece operates on quite a local scale within a research project itself, she remains concerned about the ways that these particular practices are constrained by their institutional setting.

Other studies have explored the security implications of 'dual-use' research - research with putatively positive and negative ramifications. Evans and Frow (2015) have, for instance, looked at issues around the development of 'dual use' science - that is, science which is understood to have potentially beneficial, but also threatening future uses. They have specifically explored practices of 'taking care' within synthetic biology - looking at how scientists within the discipline handle potential dual-use issues during their everyday work. The authors classify these responses as either occurring within a dual use framework or outside of it, where, in the latter case, the constructed nature of the categories of dual-use are problematised by the scientists. Once again the analytic focus here is on how locally situated actors navigate institutional environments, an interest that this research project also shares. Further, the concerns of the researchers in these situations are not too far removed from information security researchers - they are focused on the potential insecurities of particular technologies, rather than, as with Möllers, the construction of technologies for security purposes. An obvious difference with the researchers in this thesis is that their primary role is this focus on this (in)security, rather than as a problematic offshoot of their normal work, as in synthetic biology. These contributions, though, have underlined the importance of looking at scientific institutions for understanding developments in contemporary security practices, while also pointing to the breadth of potential theoretical sources for the study of security that STS offers.

3.2 Cybersecurity

In this section the range of literature considered will be narrowed significantly, and I will relate my project to debates around the specific topic of cybersecurity – a discussion that largely operates within the disciplines involved in the social study of security, science and

technology, outlined above. With this I would like two points to become clear: firstly, that academic information security research has been largely overlooked as a relevant site in social studies of cybersecurity, and, secondly, that certain STS and CSS conceptual devices are well equipped for drawing out interesting lessons from this empirical site.

3.2.1 Realist accounts

Information security, as we have seen, has been researched for some centuries, while computer security has since the second world war become a more or less institutionalised discipline, with the first conferences dedicated to the topic established in the late-1970s (Dlamini, Eloff & Elloff, 1991). Although this research has been dominated by a technical focus, social aspects have regularly emerged, with various computer scientists and mathematicians invoking certain social or, particularly, economic theories to explain information security outcomes (c.f. Odzlyko, 2003). A sizeable literature has also developed since the early 1990s from social scientists explicitly focusing on the social and political elements of cybersecurity (Dunn-Cavelty & Egloff, 2019), particularly within IR and security studies.

In this work realist theoretical approaches, based on the assumption of self-interested nation states, who are understood to struggle for power in an anarchic international order, have been prominent. The main questions that arise in relation to cybersecurity are how this new technological field impacts this balance of power, which actors will benefit and which will be disadvantaged from the technology, and what specific outcomes are likely to emerge given a cyber conflict. Generally the response that comes from realist theorists is to downplay the potential impact of cybersecurity on normal interstate relations. Gartzke (2013), for instance, attacks sensationalist media coverage of cybersecurity and aims with his work to bring discussions of cyber security 'back down to earth'. He argues that cyber conflict will mostly act in support of traditional, 'terrestrial' conflict and that the aim of conflicts will regardless remain the same. Valeriano and Maness (2015) similarly downplay the possible impact of cyberspace on interstate conflict, and claim that dominant nation states will benefit the most from these developments. They point to the high cost needed to utilise these new tools effectively as an indication that the international status quo will remain stable. The authors argue that this is the best function of realist theory for cybersecurity research - to

"temper many of the more bombastic cyber predictions" (Valeriano & Maness, 2018, p. 264). This explicitly presents a static picture of the international order, where these new technologies do not impact on the underlying balance of power between states.

This rational state model, while popular, has also been subject to a wide range of critiques. These have come from both relatively orthodox and more 'critical' perspectives, with Lucas Kello's (2017) Virtual Weapon and the International Order a particularly nuanced example of the former. He argues against a range of 'cybersceptics', forcefully claiming that cyberthreats and weapons are very real entities which have the power to upend the system of international relations. He specifically argues for the need to move beyond state centric approaches, looking at the diversity of actors in cyberspace and the means through which these actors gain power through systemic disruption. Arguably, though, Kello does not commit himself to a fully changed theoretical repertoire, staying in a surprisingly state-centric position. The text also suffers from his explicit decision to focus on the 'social' aspects of cybersecurity. Because of this, the description of the technical domain is left in a peculiar position, alternating between being opaque - cybersecurity as monolithic and undefined - and completely transparent - using technical terms as if there is no ambiguity in their meaning. The reader in this case is left ignorant of the specifics of the technologies of cybersecurity, the processes that varyingly define this domain and, particularly, the very social (and technical) worlds that are central to the construction of 'cyber' as a real and meaningful phenomenon.

3.2.2 Constructivist approaches

Others have highlighted how certain constructivist approaches to IR are particularly relevant for cyber relations, with studies particularly looking at how the (international) politics of cybersecurity is structured through the use of various linguistic conventions. Tim Stevens (2012), for instance, points to the failure of rational actor/interest based models to understand or encourage deterrence in cyberspace and how this failure has been acknowledged by the US administration. Rather a policy based on norms and ideas has emerged, with the aim of encouraging a culture of international restraint in cyberspace. Thus a constructivist approach focused on the production of collective understandings of cyberspace is well suited to understanding contemporary dynamics in this realm. In his work with David Betz, Steven's

has given a good example of what such an analysis can look like (Betz & Stevens, 2013), exploring the different analogies underpinning the politics of cybersecurity. Policy makers sometimes understand this setting as a (cyber)*space* for instance, while other times conceptualising it in organic biological terms (computer viruses), while the use of military metaphors is also prominent. Importantly these analogies are said to guide the research and practice of cybersecurity, though how this happens is not explicitly discussed. We are given a good understanding of how cybersecurity is popularly understood, but an approach to the mundane, technical practices that materialise these general understandings is not developed.

Hansen and Nissenbaum (2009) have also provided particularly interesting insights from a more critical perspective, applying the Copenhagen School's 'securitization' framework to cybersecurity. Through this they aim to show that this issue constitutes a new security 'sector' - a distinct arena where specific referent objects and threats are constructed through particular political discourses. They thus outline the diverse objects that need to be secured in cybersecurity - computer networks, states, businesses, individual PCs - and highlight how these are linked. This link is based on a relationship between two securitizing discourses, 'hypersecurity' and 'everyday security' practices, whereby the state-centric threats of the former are dependent on lay actors' mundane practices of the latter. The third securitization discourse that they highlight - technification - is particularly important for this project. This discourse makes the claim that cybersecurity is primarily a technical concern, and thus the domain of experts, rather than the public at large. As the authors state "[t]echnifications are, as securitizations, speech acts that ''do something'' rather than merely describe, and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves." (p. 1167) It is therefore imperative to challenge the apparent neutrality of these spaces, unpacking the complex politics that they are implicated in.

While this is a worthwhile text, it also suffers from a similar problem to Stevens and Betz's; the authors here again point to the importance of the practice of security, yet an empirical analysis in this direction is largely absent. Emphasis remains on the power of political discourse and we are given little insight into how these discourses are materialised. In recent times a number of approaches have begun attending to these technical practices, drawing from both Parisian critical security studies and STS.

3.2.3 The practice of cybersecurity

Simon and De Goede (2015) is one paper that highlights the worth of looking at practices constitutive of cybersecurity. They are especially concerned with bureaucratic practices in Europe and look at two central cybersecurity institutions - ENISA and ESCO. Their main contribution is the concept of 'bureaucratic vitalism', with which they hope to emphasise two points. Firstly, that cybersecurity discourses in Europe emphasise the issue's vitalism - that is, that the cyber domain is understood as a complex, unpredictable area, where process is seen as more important than being, and contingency is preferred to causality. Secondly, they aim to show how in mundane bureaucratic practices this vitalism is undercut by more traditional, rigid, structures. As they say, governance "seizes upon a notion of the incipient and unpredictable in the name of emergent governing, but ultimately requires the restoration of the transcendental script of an event and a protocol of 'right' responses that are thought compatible with crisis in the 'real world'" (ibid, p. 22). This thus highlights the need to check discursive pronouncements against everyday activities, and that the organizing effect of these discourses should not be assumed. While this study does touch on important issues, the focus is still focused on quite traditional spaces of politics, looking at how they deal with this particular issue, rather than looking at the technical spaces of cybersecurity as important sites of social activity.

Others have in recent years have drawn from STS's theoretical toolkit to do just that. Dunn Cavelty (2018) is most direct about the potential benefits of such an approach. She argues that work focusing on the social aspects of cybersecurity, both realist and critical, often takes the material and technical aspects for granted, while technical work similarly ignores social processes. She argues that STS concepts can help to bridge these two strands of literature. Balzacq and Dunn Cavelty's (2016) application of Actor-Network Theory is indicative of this approach. In this they invoke the theory's ontological framework, explicitly developed by Mol & Law (1994), where three distinct topologies are described - a predictable 'regional' or Euclidean space, a relational space of networks, and an amorphous fluid space. Using this framework the authors analyze cybersecurity, aiming to undermine accounts of the 'cyber' as a space consisting only of networks. Focusing on the Stuxnet cyber attack, they examine the ways that this malware was embedded in different sites, through which various ontologies were produced. Examples include national statistic gathering, dependent on well

defined regional space, to chaotic public reactions to the event, occurring in unpredictably changing fluid spaces, and information security technicians, conceptualised as working in a network space. This last point is worth emphasising - that those working in information security are understood as engaging in stabilization processes - moving phenomena from a fluid space and attempting to transform them so that they can be communicated and acted upon. While this article, and other of Dunn Cavelty's work, does begin to introduce information security research as important sites within cybersecurity, she does not pay sustained attention to the site, instead briefly mentioning it within a broader argument.

One paper that does explore information security in its own right is Shires's (2018) ethnography of different academic security conferences in the Middle East. He argues that such a study is necessary as "the content of computer security, and how and where it overlaps with or adopts labels of cybersecurity and information security, are themselves key areas of contest" (p. 32). Drawing on IR literature about epistemic communities, he conceptualises computer security experts as strategic actors, who try to become arbiters on the need for certain forms of knowledge. In line with this he sees academic security conferences as places through 'ritualization' computer security gets performed in that they are "more rule-governed, invariant, and formalised than the day-to-day work of cybersecurity professionals." (p. 36) Two findings are important here. Firstly, the comparison between these conferences and hacker conferences, that despite the similar focuses - malware, vulnerabilities etc. - the ritualization here produces a distinct (more formal) life world from hacker events. Another central argument is that these spaces help to partially purify cyber expertise of its commercial content, through a separation of the knowledge section of the conferences - the auditorium - from the commercial - the trading hall. While this article is close in many ways to the empirical case and theoretical approach of my thesis, the work conducted here is still a worthwhile contribution on both levels. Firstly, the everyday research lives of security professionals still remains unexplored from a social scientific perspective, something that this thesis will immediately address. More fundamentally this approach will take a more agnostic approach to expertise than that engaged in by Shires - it will, for instance, see the question of their motivation as an open one to be explored within empirical research, rather than immediately adopting an assumption of strategic motivation.

This thesis is intended to join this line of research into the practices constitutive of cybersecurity. It will contribute to them both empirically and theoretically. On an empirical

level it will expand our knowledge of a world underexplored in the extant literature: academic information security research. A guiding assumption is that this technical space is also a social one: full of rich technosocial processes that are important to comprehend the contemporary provision of (digital) security. Moreover this thesis will contribute theoretically by drawing on a novel conceptual source in the study of digital security: Luc Boltanski. This theoretical inspiration will allow for a particular understanding of practices that oscillates between the Latourian STS and the Bourdieuian CSS approach, understanding actors as both creative and constrained, and practices as both generative and determined.

4. Theoretical framework

The concepts used to guide this thesis are drawn primarily from the writings of Luc Boltanski, as well as from subsequent elaborations of his work by valuation studies scholars. In connection with this literature I want to make three arguments. Firstly, that the valuation studies can be fruitfully expanded by applying its inductive and empirical sensibility to further areas of Boltanski's research programme. In this thesis I will use three of his concepts – *critiques, justifications* and *tests* - in a way that is in line with work in valuation studies. Secondly, I want to highlight the ways in which Boltanski's approach operates between the critical sociology of Pierre Bourdieu - influential, as we have seen, within CSS - and the pragmatic approach of Bruno Latour - the main theoretical referent with STS. Ultimately Boltanski's toolkit allows one to attend to the multiplicity of moral orders within social life, while also remaining cognisant of the specific institutional settings within which these actors work. Thirdly, I want to argue that critique has been problematically addressed by both Boltanski and Latour and that there is a need for a sustained empirical analysis of the different forms that critique can take.

4.1 Background: Boltanski's intellectual history

Fundamental to understanding Luc Boltanski's thought is the evolving intellectual landscape which it has responded to. Beginning his career in the early seventies Boltanski worked as a colleague and collaborator of Pierre Bourdieu, celebrated for his programme of critical sociology. This approach, using concepts such as *field*, *habitus* and *capital*, focuses particularly on issues of social hierarchies – and "how stratified social systems of hierarchy and domination persist and *reproduce* intergenerationally without powerful resistance and without the conscious recognition of their members" (Swartz, 1999, p. 6, emphasis added). His explanation of this reproduction, based on detailed empirical studies of specific social groups, is that cultural practices and symbols help to structure society into relations of competition and hierarchy. Boltanski's (1987 [1982]) early study of the social class of cadres in France embodies many aspects of this approach - giving a detailed empirical and theoretical analysis of the ways in which this specific social group is reproduced through

symbolic and structural processes.

From the mid-1980's, though, Boltanski has emerged as a prominent representative of a new pragmatist sociology that moved away from this critical tradition. The reason for this divergence is largely related to different understandings of the proper role of sociologists and the epistemological privileges that can be granted to them. Specifically this relates to the position of social structure within critical sociology, which is understood to constrain the behaviour of actors and act as a force of domination. These forms of domination may, though, not be visible to the actors themselves ("without the conscious recognition of their members" Swartz, 1999, p. 6 quoted above) and the sociologist is here given the task of rendering these structures visible. One problem for pragmatist critics of this approach is that the domination described by the sociologist may not resonate with the lived experiences of the actors themselves. As Boltanski puts it - "what the sociologist will establish, in critical fashion, as a relationship of domination is not necessarily presented or even lived by the actors in this register; and the latter might even turn out to be offended by such a description" (2014, p. 20). Moreover, this results in those being studied as emerging as 'cultural dopes' (Garfinkel, 1967, pp. 66-75) - unreflective actors whose actions, values and reflections are determined 'without powerful resistance'. This, finally, puts the sociologist in an elevated epistemological and political position where only they have the vantage point to determine the real structures of domination, and thus also the ways that these can be contested.

Due to these issues Boltanski and others have instead adopted what they call a 'pragmatic sociology of critique'. The central change here is that the 'cultural dope' of critical sociology is replaced by the 'cultural critic' - actors are understood to be reflexive and critical within their own lives. As such social reality is rendered as a 'trial' (Boltanski, 2014, p.25), characterised by quite regular disputes and controversies, and uncertainty about normative orders is commonplace. The role of the sociologist here is to attend to these lived understandings of morality and politics, rather than imposing their own definitions onto a particular situation. The pragmatism of this approach emerges in relation to the centrality placed upon microsituations, the reflexive capacities of the actors and the uncertainty within which these actors must operate. It, though, remains focused on issues of power and domination through the centrality of the concepts 'critique' and 'tests'. The main impact of these ideas, and the research programme based on them, is to have complexified critical sociology's picture of social life. Actors and their actions, values and reflections are not

determined by their position within a social structure - rather multiple orders exist within each social domain, and any coherency created within particular situations is one that has been partially and contingently constructed by reflective actors within this site.

4.2 Sensitizing concepts

Within this overall programme there are three concepts central to its development that have also guided this thesis – *justifications, tests* and *critiques.* These will be outlined below, highlighting how they relate to various ideas within STS, valuation studies, critical security studies, as well as this particular case of information security research.

4.2.1 Justification & Valuation

The focus of Boltanski's research likely to be most familiar to researchers in STS is justification. Primarily developed within the Boltanski & Thevenot's *On Justification* (2006), this process has been central to the empirical analyses developed by Boltanski and has also been elaborated in important ways by the field of Valuation Studies.

The basic claim here is that if social life is characterised by continual disputes, actors must therefore justify their actions to each other – through which they articulate the value of their actions. Boltanski and Thevenot's allegory of serving dinner is useful to ground these ideas:

> *Let us take up a very common problem: how, in the course of a meal, to distribute the food among the guests. [...] the implementation of this order can be difficult, particularly when the possibility of a simultaneous existence of different orders of worth arises. Is it better to present the dishes first to the grandmother or to the host's boss? The possibility of protest stems from the presence, in the same situation, of different possible orders. Tacit agreement among the participants on the kind of qualities that must be emphasized by the service order is the condition of a harmonious, smooth-running scene. But the pre-condition of this agreement is a common recognition of a conventional equivalence that can support a judgement on the relative size or worth of the persons concerned.* (1999, p. 363)

Boltanski & Thevenot argue that in justifying their actions, actors must appeal to some general principle of worth which the other actors also agree - whether this be the worth of the grandmother within a familial order or that of the boss within the workplace. They specifically outline six different orders of worth within which justification can occur - *domestic, inspirational, civic, reputational, commercial* and *industrial.* According to the authors, these orders are each characterised by a specific grammar - a certain, relatively stable set of rules that operate within each world, including: the mode of evaluation, relevant information, the basic relation, and the valued qualification for humans within each. The market world, for instance, is respectively characterised by evaluation through price, monetary information, relations of exchange and humans distinguished according to their purchasing power. Boltanski and Thevenot argue that these models manifest themselves in two distinct ways - systematically within classic scientific and philosophical texts, and more sporadically in lived reality, where different worlds can be simultaneously drawn upon by the actors.

While Boltanski's model the six of 'orders of worth' has itself proven influential, (Jagd, 2011 for a review of such studies within organizational sociology), others have criticised it for being too limited and the reasoning - applying the orders of worth found within specific classic texts onto empirical situations - as being overly deductive. Fochler, Felt & Mueller (2016), for instance, say that "authors have taken up Boltanski and Thevenot's interest in studying how actors refer to figures of valuation in their practices, but they have mostly found that their deductive scheme is too rigid for the empirical study of valuation as practice" (p. 180). Instead scholars within valuation studies, influenced by the doggedly empirical and analytically agnostic approach of Actor-Network Theory, have developed a more nuanced and inductive perspective to the issue of worth and value. Boltanski's abstract reasoning, with research based on predetermined categories and distinctions, is replaced by a research programme that sees values as contingently emerging through heterogeneous practices. The concept of value is in this way further deflated, with philosophical and economic debates about the true value of objects put to one side, replaced by empirical work that teases out the complexities of the specific enactments of value within particular settings. Heuts & Mol's exploration of "[w]hat is a good tomato?" (2013) is indicative of this approach. The authors argue here, based on their interviews with several tomato growers, that Boltanski's regime isn't flexible enough to make sense of the lived

experiences of their interviewees and they "took the complexity that ensued not as an analytical flaw, but as an empirical fact about the valuing of 'good tomatoes.'" (p.129) This foregrounding of complexity leads to an approach whereby the justifications given are seen as only loosely shared 'registers' and the fluidity and contingency of these practices is emphasised.

This approach has also been used to empirically investigate certain knowledge cultures, particularly in Dussauge, Helgesson & Lee's (2015) collection of essays. This volume looks at various practices of valuation within life science research and medicine, exploring, for instance, the entangled relationship between economic valuations and other logics of value in science, the valuation of heterogeneous actors within scientific practices, and, importantly, the areas that are practised as worth knowing about within science and thus get researched. This last point is essential for my research, and the question of "what values are articulated and given weight when deciding what is worth knowing?" (p. 13) corresponds closely with my research interest and approach in this thesis. As the authors state: "the very existence of the trial certif[ies] that something had been considered worth knowing" (p.14). Importantly what is enacted is not one particular value, or a set of coherent values, but "the trial exists in a nexus of valuations that enact different and even divergent values" (p.13) to be explored in empirical research. A close examination of valuation practices in this way offers itself as an avenue into my research problem: How do research priorities emerge within the academic discipline of information security? What do researchers consider worth studying and securing? This theoretical approach moreover allows these questions to be answered in a 'person centred' way (Fochler, Felt & Mueller, 2016). That is, that the emergence of research within particular disciplines is not viewed as some disinterested, mechanistic phenomenon, but rather as part of "how individual researchers navigate and cope with the complex realities of contemporary research landscapes." (ibid, p. 180)

4.2.2 Tests, Heterarchies & Regimes of Valuation

The second aspect of Boltanski's theoretical apparatus that this thesis will utilise is *tests*. Tests are essentially situations where the relative worth of various people, things or actions are evaluated and institutionalised or "the selection process governing the differential distribution of persons between positions of unequal value" (1999, p. 32). This broad notion captures a wide variety of different mechanisms - from job interviews and college entrance

exams, to border controls and wars - that involve this evaluation and ordering of worth. Tests are thus characterised by relations of force: while many different actors may have views about the relative worth of humans and objects, only certain actors have the power to implement tests that actually distribute actors according to some particular order of worth. Important then is that tests are a central material realization of justifications and the principles of value they are based upon - if justifications are processes where a moral order is discursively constructed, tests are the central mechanism through which these justifications come to shape the actions of actors within them. Focusing on tests thus helps to situate the processes of justification within specific institutional contexts, and indicates ways that particular understandings of value become dominant at certain times and places across society. One way to make this clearer is by viewing them as a response to the claim that *On Justification* was problematically relativistic. While the book highlighted the multiplicity of the possible normative principles that ordinary actors could appeal to within their disputes, it did not give any analysis of historical regularities in terms of valuation practices. This Fowler (p. 71 refers to as the text's "disturbing kaleidoscopic perspectivism". For Boltanski *tests* help to explain order and stability within social life, and gained prominence in his next major work, *The New Spirit of Capitalism* (2005 [1999]).

In this book he and Eve Chiapello argue that capitalism has had three distinct phases, and that each of these stages has been characterised by a particular logic of worth – the first being a compromise between the commercial and domestic worlds, while the second was a compromise between the industrial city and the civic city. What is important for Boltanski is that these justifications are not superficial ideologies that cloud the true nature of capitalism, rather they change its very functioning, primarily through the establishment of different sets of tests that help to arrange society according to different logics of value. Boltanski goes as far to say that it is "no exaggeration to think that a society (or the state of a society) may be defined by the character of the tests it sets itself, through which the social selection of people is conducted, and by the conflicts over the more or less just nature of those tests." (ibid, p. 32) Thus, again, it is through tests that particular logics of worth are seen to be established across different parts of society.

While scholars from valuation studies are generally averse to structurally deterministic accounts of the emergence of valuation, certain scholars have tried to theorise about the ways in which specific valuations become relatively dominant in certain times and

spaces within social life. As Dussauge et al., for instance "caution against the complete analytical naivety proposed by certain pragmatists (cf. Latour 2005) who tend to disregard the historical regularities of society" (p. 9). One way that this has been done is through the opposition between *hierarchy* and *heterarchy* introduced by David Stark (2000). The idea here is that in sites characterised by hierarchical ordering of values, one understanding of value (economic, domestic etc.) tends to dominate, while in heterarchical orderings, multiple notions of value are considered legitimate. Stark advocates for the adoption of these heterarchical modes of organization as leading to a more resilient and creative organization capable of adapting to a changing environment. Another notion that tries to capture the institutional dimensions of value practices is 'regime of valuation' (Fochler, Felt & Mueller, 2016). This refers to the "discursive, material and institutional background [a] concrete evaluation draws on" (p.180). These regimes are thus relatively coherent and institutionally embedded sets of value practices that impact on actors' own valuations in some way.

While these ideas are interesting, and will be engaged with in subsequent chapters, this enquiry begins with the notion of *test.* The specifically broad nature of this category allows for an inductive analysis, exploring which tests are important for my researchers in which ways, slowly building a complex image of the institutional environment within which the actors are situated. It allows one to leave open questions regarding the legitimacy and effectiveness of tests, as well as the presumably quite complex orderings of value within all social sites, including the research centre. That said this thesis will not directly apply the Boltanskian framework of tests onto the empirical site of SBA research. Once again the analytical divisions made by the French theorist remain too abstract and too rigid to be useful within empirical fieldwork. The concept of test will again be treated in line with sensibilities drawn from valuation studies, trying to analyze these in an inductive and empirical fashion, developing analytic distinctions through engagement with the case itself.

4.2.3 Critique

The third central focus in Boltanski's work that this thesis will adopt is *critique*. Critique itself is a notion that has been central to a wide range of post-enlightenment philosophy and social thought, (c.f. Foucault, 1984), with a large amount of different understandings of it developed. It has also been approached from quite novel perspectives by Boltanski and Latour, as well as subsequently by scholars in STS and CSS, perspectives which also diverge

from each other in important ways.

The notion of critique has, as we have already seen, a central place in Boltanski's research programme. This programme, called the sociology of critical capacities, understands actors as being reflexive and the social world as comprised of disputes and controversies. Thus a central process within this is the various claims that actors make about each other's behaviour and their general situation - their critiques. In *On Justification* the authors argue that each order of worth also has a related critique directed at the other orders. The inspired world, for instance, criticises the rigidity of the industrial world, while the market world sees the domestic world as corrupted by personal connections. In *The New Spirit of Capitalism,* the role of critique in producing social change is underlined. The authors concretely argue that critiques of capitalism have led changes in the spirit (justifications) and functioning (tests) of this economic system. The two central forms of critique that have been historically prominent are 1) a social critique of the suffering that capitalism causes and 2) an artistic critique of the boredom it induces. They look at the emergence of the new spirit of *projective* capitalism as primarily a response, and co-optation of, the artistic critique which has been dominant since the 1970's. In more recent years Boltanski has focused further on the role of critique in society, examining the ways in which his research programme can help to strengthen the critical capacities of actors (2011 [2009]).

These ideas have a somewhat complicated relation to Bruno Latour's approach to critique, epitomised in his famous polemics about it 'running out of steam' (2004). The argument in this piece certainly shares characteristics with Boltanski's approach: Latour also tries to distance himself from the critical sociology of Bourdieu and his colleagues, again arguing against the privileged epistemological position of sociologists. He specifically claims that their reliance on both positions of relativism and realism is conceptually muddled but also strategically wily - the sociologist in this situation can never be wrong. Both authors also claim that an empirical research programme focused on the complexities of the lived world should replace this traditional form of sociological critique, with Latour proposing the investigation of *matters of concern* as his preferred response. This is an analysis of the heterogeneous practices that allow for the emergence of various objects and realities, in line with ANT's general orientation. Latour though goes further than Boltanski and argues for a re-conceptualisation of critique *per se.* That is, certain 'debunking' critical activities are in general referred to as 'barbaric' and in need of being replaced by more positive critical

gestures. Justifying this he refers to certain conspiratorial activities of non-academic actors, comparing these to the repertoires of critical sociology: "What's the real difference between conspiracists and a popularized, that is a teachable version of social critique inspired by a too quick reading of, let's say, a sociologist as eminent as Pierre Bourdieu [...]?" (2004, p. 228). The conclusion is that both academic and non-academic forms of critique should be changed. "Is it not time for some progress? To the fact position, to the fairy position, why not add a third position, a fair position?" (2004, p. 243)

Regarding this 'fair position' though Boltanski and Latour diverge in important ways. While they agree about the need to deflate the role of the sociologist as critic, Boltanski clearly values the role of strong critiques within both academic thought and social life in general. As Guggenheim and Potthast (2012) put it, "while [Latour] has opted for radically flattening out critique, [Boltanski] maintains that critique requires an external point of view, which has to be determined by pragmatist analysis." (p. 13). Indeed, Boltanski sees the primary role of his thought to be to strengthen critique in society, while remaining committed to emancipation as a political end. In light of this, Boltanski has moreover recently given a critical evaluation of his own pragmatic programme (2011, p. 29-33). Here he claimed that while the pragmatic school of French sociology has been useful in highlighting the moral capacities of ordinary people and bringing these capacities into sociological thought, it has also been found in these studies that ordinary actors relied upon critical social theories focused on domination in their own critical activities. By exclusively offering pragmatic studies, sociologists risked shrinking the critical repertoires of actors engaging in various types of political struggles and thus weakening the power of critique in society.

These issues have also been dealt with by researchers within STS/Valuation studies and critical security studies. Within CSS, for instance, a recent edition of the journal *Security Dialogue* was dedicated to the topic of critique and it elicited a number of quite diverse responses to this issue. One theme was quite common - a re-conceptualisation of the practice by employing ideas related to STS. The lead editorial is most explicit in this (Austin, Bellanova & Kauffmann, 2019), arguing that this re-conceptualisation is needed because of a current malaise in critical thought, related primarily to its inability to actualize change in society. Responding to this they argue for "an embodied account of critique that reveals how it comes to matter, or not, practically speaking. To meet this challenge, we focus here on what we term the 'doing' and 'mediating' of critique" (p.4). They draw from Donna Haraway

to argue for a form of companionship in critique, where the collective constitution of critique is focused upon - critiques are understood to be the product of a wide array of heterogeneous relations. This allows the role of the sociologist to be reconfigured as a mediator of critiques within a broad and heterogeneous landscape.

Concerns similar to Boltanski's have also, though, been recently voiced by valuation studies scholars. Concluding their volume of valuation in the life sciences, which took matters of concern as a central starting point, Dussuage et al. (2017) in general argue for analysts to again take a more interventionist stance in relation to their research. They again worry about "the risk that a pragmatic and emic approach might provide insufficient resources to allow actors to perform a substantial critique" (p. 281). They give several possibilities of the form that this intervention may take, from mediation towards a more activist approach. This interventionist understanding of research is also related to moves within STS to *experimentalize* research methods. Here again Boltanski is a central reference, with Guggenheim (2019), for instance, arguing that these methods are trying to proactively enact the disputes that the French sociologist explored, and that through this the critical spirit of ANT can sustain its steam.

Having these discussions in mind, this thesis will begin on a note of ambivalence regarding the value of different forms of critique. On the one hand Latour's diagnosis of the abuses of critique is important to bear in mind - particularly given the subsequent growth in post-truth politics (c.f. Fuller, 2018) - and Boltanski's undifferentiated support of critique in and of itself seems inappropriate to this. On the other hand concerns about a purely pragmatic approach weakening the critical capacities of vulnerable actors seem also plausible and chime with consistent criticisms of the political implications of ANT. How then to proceed? One way forward seems to be, following the researchers from STS and CSS, through an empirical analysis of the different forms that critiques take in specific sites within society. Looking at the critical strategies of all actors, regardless of our sympathy for them, seeing what political impact different critiques can have, and beginning to think about our own critical activities on this basis. This thesis will be a step towards this; by looking at information security researchers as critical actors it will try to understand the different types of critiques the researchers formulate and the way in which these become institutionally embedded, without any preemptive evaluation of the merits of critique in general. This empirical and inductive approach is once again in line with sensibilities developed within STS and valuation studies,

and with the overall theoretical approach utilised for this thesis.

5. Research questions

Up to this point of the thesis the general empirical case has been outlined, a range of literature that relates to this issue discussed, and a specific theoretical frame with which to approach it developed. Based on this I have developed several research questions (one main question, and three sub-questions) which have guided the subsequent empirical research. These will be described in this literature, pointing to their connections to

5.1 Main research question

My main research question is:

> *How do PhD researchers in SBA research present the emergence of research concerns within information security research?*

In answering this question I want to try to directly explore the central social process that I am concerned with in this thesis: the emergence of research concerns within SBA research. While apparently mundane, it is also, I contend, related to important and prominent issues, and will ultimately help to elucidate the complex interrelations between practises of science, technology and (cyber)security.

My interest in this question can first be situated within discussions around the topic of cybersecurity, prominent in the media, in the social sciences and within information security research itself. A common concern within these discussions is the rapidly expanding number of devices connected to the internet, and the manifold information security implications of this development. As Bruce Schneier (2017) puts it: “The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in. This is the future, and what we're calling the Internet of Things” because of which “what used to be a specialized area of expertise now affects everything. Computer security is now everything security.” Faced with such a situation of perceived expanding complexity, it is important to engage with processes of prioritization, decisions about which topics to focus upon, what areas to secure, and to see these as sites of contestation. Put simplistically: Why

should the hospital or the factory be the focus of research? How does Blockchain become such a prominent focus of the discipline? What is the specificity of the researchers' work and how does this emerge? This thesis will centrally be an exploration into how these researchers delve into and make manageable this complexity, how they justify their decisions and the institutional structures that are involved in this process.

My interest in this process is further based in literature from critical security studies. It was seen in the literature review that a central concern of this field, particularly for the 'Paris' school of thought, was the empirical investigation of the practice of security within distinct social worlds constitutive of a broader field of security. Research within critical security studies has thus increasingly focused on "the boundaries and definition of the term "security"" (Bigo, 2006, p. 24) within the practices of various groups related in different ways to its contemporary provision. A central assumption of this thesis is that information security research is in *some way* a space of security, and that the central way that this security is practised here is through the research conducted in the centre. Thus, the practice of a distinct form of security and the prioritization of different threats (and referent objects) emerges through the particular research focuses present within the centre. It is therefore imperative to critically analyze the different forms that this research takes and the way these come into being, to give an empirical account of the security practices in this so far understudied site.

The question then becomes about how different focuses emerge within research. To answer this question is complex, though, with different theoretical perspectives offering alternative explanations. One recent approach, though, has been the use of valuation studies to understand the constitutive practices of various knowledge cultures. Following this approach, and particularly Dussauge, Lee & Helgesson's (2015) application, I am viewing research as sites where values are enacted through practices. A central part of this is the specific type of research that gets conducted and the specific values that this enacts. As the authors state: "the very existence of the trial certif[ies] that something had been considered worth knowing" (p.14). Importantly what is enacted is not one particular value, or a set of coherent values, but "the trial exists in a nexus of valuations that enact different and even divergent values" (p.13). This thesis will thus look at the emergence of research concerns, and thus of a particular form of security, as related to heterogeneous enactments of value. Following Luc Boltanski, three sets of enactments have guided empirical research:

justifications, tests and critiques. The following three sub-research questions will also each be based on one of these concepts.

5.2 Sub-question 1

The first sub-question is:

How do researchers justify the value of their research?

With this question I want to focus on the first set of value enactments that will be explored in this thesis: justifications. As we have seen, Boltanski has underlined the importance of justification as a social process – seeing it as a way through which notions of value are articulated and negotiated. Focusing on this process within SBA Research will thus give a sense of such an order here, looking specifically the different ways that research can be seen as valuable and the various resources that the researchers can draw upon to make this case. I am also here directly following the methodology prevalent within valuation studies, particularly that of Heuts & Mol (2013), which makes Boltanski's understanding of justification more flexible to varying empirical situations. The analysis will thus try to be more inductive in character, with analytic distinctions emerging through the process of empirical research.

One theoretical contribution of this thesis is to argue that through an examination of security actors' justifications of their work, the referent object of this work emerges. That is, the actors justify this work according to the security it will provide for a particular actor, group, object, or process, and thus we get an insight into who this particular security practise is intended to serve. This particular theoretical framing further helps to see security here as a generative practice. Security in information security is not, in this view, a shared definition of the key term, or a practice determined by a position within a social structure, but it instead emerges through multiple enactments of worth. Attention will be paid to the multiple and heterogeneous justifications given by the actors, as well as how these are articulated within specific episodes of interaction.

5.3 Sub-question 2

The second sub-research question will be:

> *How do researchers present the 'tests' that evaluated their work and their impact on the development of their research?*

This question is based on Boltanski's concept of tests – which are repeated events through which objects and persons are ordered according to a particular understanding of worth**.** With this question I will try to develop a nuanced understanding of the institutional environment that the researchers operate within, and how this environment contributes to the overall question of the emergence of research concerns within information security. Thus, while the previous sub-question emphasises the multiplicity and contingency of practices within this particular security world, this sub-question will allow for this to be tempered with an understanding that these practices as also constrained by broader institutional forces, albeit in a complex and non-obvious fashion. This will thus offer some steps towards explaining historical regularities of security enactments within information security research.

I also want to attend to the *specific* experiences of researchers within this research situation, and avoid making a priori assumptions about the overall structure of evaluation, such as in certain debates around new public management and neoliberalism. Instead I want to look inductively at what specific tests the researchers are subjected to, what values these tests attempt to enact etc. Important, also, is that the question of the exact role, legitimacy and impact of the tests is left open at this stage. One possible result of this research will be the identification of a regime of valuation (Fochler, Felt & Mueller, 2016) - a coherent institutional background which a particular valuation draws upon etc. - but the identification of a coherent regime is not guaranteed. This question thus offers an avenue of looking at the broader situation of the researchers, while remaining committed to the primacy of their own perspectives.

5.4 Sub-question 3

The third sub-question will be:

How can the critical activities of the researchers be conceptualised?

This question focuses on the third of Boltanski's concepts that will be used: critique. Here researchers will be broadly conceptualised as critical actors, and it will be assumed that they engage in critiques both within their professional and personal lives, and, in the interview itself. This first part of the question – the professional critiques - is closely connected with the first research question - the interviewees' presentation of their work. That is, it will be assumed that at least part of the impact of the researchers work will be a critical assessment of the behaviour of various actors. One important contribution of this research question is to situate this alongside critiques made by the actors within the interview situation itself, and to tease out the differences between these institutionally embedded and isolated forms of critique within the analysis.

This further helps to contribute to discussions around critique, centred on the ideas of Luc Boltanski and Bruno Latour. As we have seen, these two authors have quite opposing approaches to the topic – the former viewing critique as an almost universally positive phenomenon, while the latter argues that only certain forms of critique should be seen in a positive light, and that many contemporary forms of it are problematic. This thesis will try to contribute to these discussions by first taking an agnostic empirical approach to the issue. Rather than offering another theoretical position on the matter, I will instead proceed with an empirical interrogation of the various forms that critiques can take, their imagined functions and implications, as well as the institutional arrangements that support particular forms of critical activities. This finally then allows for reflexive discussion to emerge about the critical activities engaged in by researchers in SBA Research, my own critical practices, those engaged in by scholars within STS and CSS, how these relate to each other, and, finally, how these might be fruitfully developed in interaction with each other.

6. Methods

This chapter will be dedicated to the methods employed to answer the research questions – looking at the concrete way that this research was conducted and the considerations taken while doing this. I will begin with a reflexive section, looking at my own position in relation to the field, being studied, focusing on my particularly external position to it, and how this influenced my research. I will then focus on the central role of interviews within this project and how these interviews, and the data they generate, are conceptualised. Lastly the chosen form of data analysis – grounded theory, supplemented with certain tools from situational analysis - will be described.

6.1 Reflexive considerations

My own journey into the field of security research is a fairly haphazard one filled with various contingencies. To begin with, I became interested in STS approaches to security following time spent volunteering in a refugee camp in Serbia, which subsequently inspired a seminar paper on conceptualising the different technology apparatuses in operation there. Perhaps due to this I am drawn to this overall topic because of particular political concerns about contemporary developments in security practices, and the analysis provided in this thesis cannot be separated from these concerns. I subsequently took two classes focused on security which solidified my interest in the area, and particularly in developments within critical security studies and the value of interactions between these and approaches from STS. The other main source of external inspiration for this project comes from my interest in digital life. I have also for a long time been interested in and concerned with developments in relation to digitalization, data politics and the problems with security that emerge with this, but only in a quite distant and indirect fashion. I find the field fascinating and important but I have next to no technical background, no knowledge about information security research, and definitely no elaborate plan for the investigation of this site. Rather my encounter with information security research came about quite coincidentally – while discussing my ideas for research about security relevant technologies, a peer talked about her place of work as somewhere relevant in this regard, and subsequently suggested I could do my research about this site.

This trajectory into the field is important as it led to quite a specific approach to the project and overall research process. I had little to no prior interaction with information security research, and thus only very vague preconceptions about the kind of work carried out here, a position which undoubtedly has drawbacks but also certain benefits. One negative effect of this relation to the field is that some of the findings are, perhaps, obvious to those who spend their lives here. While for me it was surprising, for instance, that a lot of research within information security could be conceptualised as a 'critical' activity, when I raised this to my last interviewee the phrase he repeated most often was 'of course'. I also have struggled to identify a regime of valuation within the findings, which is perhaps due to a lack of prior knowledge about the field and the institutional environment within which it is situated. On the other hand my relative ignorance fits the inductive approach outlined within the theory section, above. I had, for instance, no knowledge of the tests that exist within this site, and could really develop an analysis of these based on my material, rather than any conceptualisations developed prior to research. Further my relative naivety within the field I think allowed me to offer a novel view on certain taken for granted elements within the field. This is reflected in Isabelle Stengers' notion of 'the idiot' - who 4) who "resists the consensual way in which the situation is presented" (2005, p. 9) as a result of their ignorance. While the finding that their work is critical, for instance, may not be surprising to researchers here, the potential of such a conceptualisation, and its relation to various strands of social thought, might not have been noticed. Through writing as an outsider from the social sciences I hope I can bring a fresh perspective to what may appear mundane to those within the field.

6.2 Field access and exploratory phases

This section will explore the process involved in gaining access to the field site and early explorations of literature directly related to this site. Particular attention will be paid to the influence of my 'gatekeeper' to the development of the research process.

As discussed above, my access to the researchers in SBA came about exclusively through a contact of mine who worked in the centre. This person thus acted as a 'gatekeeper' for my research. Gatekeepers are people who, according to Sabine Tuning (2015), help with "an introduction into a new field of research" and "who 'guide' the researcher to new contacts." Luning further argues that it is important to acknowledge the role of a gatekeeper in the development of a research problem, referencing Marilyn Strathern's idea that research

is formed ‘in company’. On a practical level, having a gatekeeper was helpful in relieving an enormous amount of administrative work. She told me, for instance, that it was better not to contact the head of the research centre to request access to their staff; rather my contact directly wrote to various groups of researchers looking for participants. More fundamentally though, my early stages of exploratory research and thus initial impressions of the site were also guided by our interactions. Most formally we had one exploratory interview where I presented some preliminary ideas, and she responded with her thoughts. Important in this was, for example, the weight she placed on the complex moral environment that the researchers operate within, discussing the various ethical (and institutional) dilemmas that the researchers face, which undoubtedly shaped the development of my research. Further her recommendations of literature and potential focus points were immensely helpful in the early stages of the research, as were her critical comments during the later stages.

While having SBA Research as a focus point for my work was useful in narrowing the framework of the project, the research centre remains a large and complex site. For some time I struggled with the question of how to narrow my focus further and to decide which part of the research centre was suitable for such an investigation. This phase was marked with an exploration of various publications by scholars associated with SBA Researchers available on their website. This was useful to get a better sense of the work carried out within the overall discipline, as well as to develop a theoretical framework and a number of research questions relevant to the site. At the same time, this provided insights only into the type of research that was conducted in the centre, and not so much the processes that allow for its emergence, which, based on my exploration of critical security studies literature, had become my primary research interest. It was thus clear at this stage that interviews would be necessary to answer my research questions. Furthermore, any decision to focus on one particular group seemed rather arbitrary at this time. Perhaps due to my lack of background in information security none of the areas seemed that clearly defined or striking, and I found myself getting lost in the different strands of literature. In the end, my gatekeeper once again proved invaluable, and she advised me to take a rather general approach and to interview researchers from three areas that were at the time prominent in SBA - blockchain, the internet of things and usable security. These groups were then contacted and six researchers expressed their interest in taking part in my study, whose subsequent interviews were the main empirical material for this project.

6.3 Description of interviewees

The central source of empirical data for this thesis are six interviews I conducted with researchers within SBA Research. Here I will contextualise the subsequent findings of this project with some details about this group, traits they share as well certain individual features, pointing to their relative specificity as a research sample.

This group of interviewees is, on the one hand, in certain ways quite homogeneous. Each of them are, of course, information security researchers employed in SBA Research. Importantly also, they are all pursuing their PhDs in information security - they are all at more or less the same stage of their careers within SBA, and are thus subject to quite similar institutional requirements. Fochler, Felt & Mueller (2015) also argue that PhD students engage in different valuation practices than later researchers, and that PhD students practise a broader array of these that are less determined by purely institutional requirements. This is an important qualification to have in mind when thinking about the generalizability of these findings, particularly that around the multiplicity of justifications they offer for their work. Furthermore these researchers are all Austrian, they are all white, and four of the six are male, perhaps mostly suggestive of the demographics of the research centre. Finally the researchers all volunteered to be interviewed. This can definitely indicate that these actors may share other dispositions and interests (relevant particularly in relation to the actor's 'critical capacities') but there was no practical way to avoid this.

In other ways, though, this group is rather diverse - most importantly in relation to their research interests. Here I will give a brief description of these, using the pseudonyms that I have given to each interviewee. These pseudonyms will be used throughout the findings section and are preferred as it retains a certain 'person-centredness' that can be lost with, for instance, numerical designations. The inverted commas around the pseudonyms will be dropped after this introduction.

I talked to three researchers who study *usable security* research. This research is concerned with how a given technology or protocol is used and the implications of this use for a device's security.

> "*Laura"* whose PhD research had so far involved looking at the use of HTTPS by administrators and end users. She had previously studied a Master's in computer science,

"Julia" who studied the usability of hardware security, and has a background in computer engineering.

And "*Simon"* who positioned his work as between this field and blockchain; he had previously also studied usable applications of privacy enhancing devices, while his background was in computer graphics.

I also talked to two researchers who focused on the *Internet of Things*, focusing on the security of these devices.

"*Markus*" focused on conventional or consumer Internet of Things. His background was in computer science and he was also the only one who I spoke with who positioned himself as coming from the hacker community and

"*Lucas*" focused on the Industrial Internet of Things – applications of interconnected devices within production processes. His background was with computer science and also law, and he positioned himself as more focused on the industry than other researchers.

I also spoke to one researcher exploring blockchain technologies – the distributed ledger mechanism that underlies bitcoin

"*Sebastian*" focused on bitcoin in his research, and the Nakamoto consensus protocol that underlies it. He has studied information security since his bachelor.

This group of interviewees is thus quite particular in some ways, while also being internally diverse, perhaps presenting a difficulty for the generalisability of the results in this thesis. Which indeed it does. This research is primarily interested in the specific and multiple valuation practices that these researchers themselves engage in, and the immediate institutional environment within which these practices are situated, rather than any comprehensive epistemic culture. Yet these results remain useful. My approach hopes to be person centred and to highlight the rich and complex practices engaged with by these particular people in distinct situations. In general in this I am informed by a sensibility derived from anthropology and ethnography, captured in Geertz's (1973) notion of 'thick description' - where the context of an actors actions, as provided the actor, becomes the centre of analysis. Thus I hope my research captures something of the complexity of the specific life worlds of my interviewees, as well as their constructions and evaluations of these.

6.4 Interviews

The central way that data was gathered for this thesis was through six semi-structured qualitative interviews. This section will provide some details about how these were arranged, and how the situation and the data generated are conceptualised.

For the thesis I conducted six interviews. These were all between 40 minutes and one hour. These interviews were semi-structured and predominantly consisted of open ended questions. This type of question was preferred for the richness of answers which they tend to lead to. As Byrne (2004, p. 182) puts its: "Open-ended and flexible questions are likely to get a more considered response than closed questions and therefore provide better access to interviewees' views, interpretation of events, understandings, experiences and opinions." One of the main practical lessons I learnt during this process was the value of and the skill involved in asking open ended questions. I found it quite difficult to formulate these questions initially, and in the early interviews I sometimes spontaneously rephrased the questions into closed yes/no ones. It became obvious throughout, though, that as I learnt to ask more open questions the breadth and complexity of the answers generally increased. Semi-structured interviews were also preferred due to the mixture between structure and flexibility that they offer - they help to make sure that the research questions can be answered, but also allow for freedom in responding to unexpected issues that may emerge within the interviews. (Jensen & Laurie, pp. 175-80)

In the interviews I used my interview guide in a rather loose fashion, with the order and exact wording of questions changing during the interview. The interviews though follow a general structure: introductory questions were asked first, followed by more precise questions about the researcher's field of interest and their work, zooming out to then look at the institutional context within which they worked, finally addressing broad normative questions about the direction of information security and the implications of this for my research. I also continually adapted this interview guide throughout my process of researching, attenuating as new ideas emerged both within the interviews and also in their analysis. (Jensen & Laurie, p. 183)

More abstractly I have followed Silverman's (2015, p. 169) conceptualisation of interviews as *interactional accomplishments.* That is interviews are not here primarily understood as giving any objective insight into some external social world – rather they are

understood as artificial contrivances where the interviewer and interviewee collaboratively produce an account of a given topic, state of affairs, life world etc. This leads to a constructivist understanding of material generated within the interview, where the data is primarily understood to be a reflection of the interaction that emerged within the interview itself, and this interaction is thus the focus of analysis. In this way distortions between the interviewees accounts and some reality is not a problem relevant in this understanding - simply exploring the ways in which accounts are formed is central. Importantly, this conceptualisation of my research material resonates well with the sensitizing concepts used for this thesis. Boltanski's grounding in a pragmatist theory leads to concepts that are deeply with a constructivist epistemological stance. For instance, critique is seen as an interactional process, and in interview settings the interviews we are able to collaboratively engage in social interactions where certain critical capacities of actors emerge. Likewise with justification: this is a process that emerges within interaction between different actors, where one actor is put in a position where they must outline the perceived worth of their actions. Thus these valuation practices are directly accessible in the context of an interview.

More difficult to get access to are tests: events where worth is distributed institutionally, which, of course, mostly happen outside of an interview. Thus, while we are interested in the evaluations of these tests performed within the interview itself, we also must to some degree trust the interviewees accounts as a fair reflection of the world outside of the interview. This is the same with certain critical activities that the researchers describe engaging in outside of the interview. The basic problem here is one of doing a praxeological interview – where the data is a description of practices engaged in by the interviewee in their everyday lives. This is a problem that Heuts and Mol (2013) reflect upon in their paper about the different valuation practices surrounding tomatoes:

> *The aim of the interviews was to learn about valuing tomatoes in practice. Ideally, we would have wanted to do fieldwork and follow our informants in all their tomato related activities. This, however, wasn't easy to achieve in our practice. We had little time, wanted to know about diverse practices, and found that potential informants were not keen to be shadowed, either because this sounded intrusive to them, or because they did not want to negotiate it with their bosses.* (p. 128)

I would explain this thesis's shortcomings in similar terms: that within the scope of this master's thesis, and given my level of knowledge about information security (and of the German language), an ethnographic investigation of the valuation practices carried out within the research centre would have simply been infeasible. Dealing with this difficulty I also followed these authors' advice: "persistently ask questions about the specificities of activities that informants tend to take for granted" (ibid), in this way encouraging these practices to be de-naturalized, and for rich accounts of them to be generated within the interview.

6.5 Data Analysis

While aware of the problems with an overly linear presentation of research, this section will focus on what was putatively (and mostly) the final stage of the research – the analysis of the data produced within the interview. This was mainly based on the framework provided by grounded theory, with the addition of some mapping techniques loosely inspired by situational analysis.

The analysis of data conducted for this master thesis largely followed the framework of grounded theory, particularly the constructivist variant outlined by Kathy Charmaz (2014). These ideas are grounded in and extend certain principles of the original grounded theory approach, developed by Glaser and Strauss. This approach was primarily driven by a desire to move away from overly theoretical and deductive explanations of social life, based on the abstract conceptualisations of, for instance, Merton's structural functionalism. Instead grounded theory was intended to move analysts closer to the empirical situation, encouraging an inductive approach where explanations of phenomena are incrementally constructed through the close comparison of empirical material. Another characteristic of this approach is that it is relatively systematic: Glaser and Strauss wanted qualitative research to become a more legitimate source of knowledge about the social world, at a time when sociology, particularly in the US, was increasingly dominated by quantitative methods. As such grounded theory presents concrete steps for conducting an entire qualitative research project, making the process more transparent and, they argue, scientific. Charmaz's particular approach is generally in line with these ideas, but with slightly different emphases. In general, she is critical of the underlying positivistic assumptions and overly rigid structuring of grounded theory. One of the central changes is simply the attitude the researcher takes to

the framework: it should be seen as a collection of heuristic devices to be flexibly experimented with to produce increasingly analytic accounts of social processes, rather than a prescribed package that allows the researcher access to a reality external to them. A more concrete shift concerns the relationship between analysis and theory. Early grounded theory advocated a purely inductive approach where conceptualisations should arise only from the data gathered - Charmaz and other constructivist grounded theorists emphasise how this is both infeasible and undesirable - and that they should be loosely engaged with to provide interesting interpretations of the processes at hand.

In this project I generally followed Charmaz's advice: using the basic techniques provided within the original formulations of grounded theory but approaching them as useful devices to produce analytic categories. I also used the chapters in her *Constructing Grounded Theory* as a general reference for each of the techniques, while I used Atlas.ti for the most part. Specifically, I close coded each of the interviews - initially on a line by line basis, but this got somewhat broader for the later interviews. Comparative coding was then conducted, where different sets of data from different interviews, and the codes applied to them, were compared with the aim of constructing more abstract categories. When new categories were formed they were tested against the rest of the data, to see in what way and to what degree these helped to make sense of the data, empirically clarifying particular conceptualisations, and trying to remain attentive to the richness within these various categories. Throughout all of this process I continually wrote memos, where the connections between the different concepts, and their connections with different parts of the data, different areas of literature, were loosely written about. I also constructed a number of "messy maps" that performed a similar function to memos, helping to continually rearrange the ideas with regards to each other, playing with ideas and categories creatively, with the aim of ultimately developing a more analytic understanding of the material.

My project though did not meet the requirements of grounded theory in one important way: it was not very iterative. As outlined above, I was given contacts to all of my interviewees at once, and this happened in a fairly random way not guided by any theoretical construction, nor by any previous analysis of data. Thus theoretical sampling, which is argued to be one of the core elements of a grounded theory approach, was not engaged in. One part of the thesis was rather iterative – my last interview happened after a gap of two months, during which I conducted a large part of the analysis for the thesis. Doing this I got a sense of

the benefits of such an approach - the questions asked in this interview were more tightly honed than at the earlier stages, and I could even, after being prompted by the interviewee, present something of my analysis at this point. One obvious way to extend this research would be to engage in theoretical sampling, which would undoubtedly lead to a richer picture of information security research.

7. Findings

In this chapter the empirical findings of the thesis will be presented. Here I will present my answer to this thesis's main research question: the emergence of research concerns within information security research. This answer will be arranged according to the three sets of value enactments that my sub-research questions are based on: critiques, justifications and tests. First, the researchers will be conceptualised as critical actors, and the various critical activities that they engage in will be outlined. Within this, their research itself will be understood as a practice of critique, and each of the interviewee's different research focuses will be in turn looked at from this perspective. These will then be contrasted with non-institutionalised critical activities that the researchers also engage in, to help to situate their research and to understand the specificity of the discipline of information security, as well as noting certain ambivalences within this study. The rest of this findings section will explore the conditions within which these critiques emerge, to try to see what lends the researchers' work its specific character. I will first look at the justifications the researchers offer for undertaking their work, separating these into various 'registers of valuation' - sets of practices that attribute worth to things relatively coherently (Heuts & Mol, 2013). I will then address the specific institutional environment of SBA research and the tests that the researchers work are evaluated through, analysing the ways that these tests are supported and contested by the researchers. Together this should give a detailed view of the heterogeneous value practices within SBA research, and the specific forms of security that emerge with this.

7.1 The Critical Capacities of InfoSec Researchers

This first part of the findings chapter is centred around the notion of critique. Specifically, the interviewees - six information security researchers - will be understood as critical actors and their critical activities will be foregrounded. Critique here is understood in a broad way as an activity where actors "review their own actions or those of others in order to make judgements on them" (Boltanski, 2011, p. 3). In this section two distinct sets of critiques will be outlined. Firstly, those that emerge through the interviewees' research will be addressed, which will cumulatively lead to understanding academic information security itself as largely

a practice of critique. Secondly, critiques that are in various ways distinct from academic information security research will be outlined, including certain activities carried out by the researchers in their private lives, as well as critiques that emerged within the interview situation itself.

7.1.1 Information security research as a practise of critique

The critiques that emerge within the interviewees' research in SBA will be the first to be outlined. The overall argument here is that a large portion of their research is critical in nature and, furthermore, that this critical activity is quite a specific one. An indication of the prominent role of critique within the research is seen in Julia's (Interview 3, May 2019) general description of the work carried out in SBA Research:

> "*I think we are always doing the first steps so major differences can be made. But you first have to discover what is going wrong, then you have to propose certain ways".*

Here we see that an evaluation of 'what is going wrong' is one central aspect of the work that the researchers do, a part of the research that will be foregrounded in this section and, in general, thesis. While this is clearly a reduction of the research carried out, with the more positive proposals under-emphasised, critique remains a fundamental aspect of the work that is shared by all of the researchers. When presented with this perspective on their work, Sebastian, who was my last interviewee, laughed slightly and said that it is a "good analysis" because:

> *I guess the main tool of people in IT security research is proof by counterexample which is when someone says this is secure and this works and you provide a counterexample of it does not.* (Interview 6, October 2019)

Here 'counterexample' is the term used to describe the negative function of the researcher's work – highlighting how, in certain situations and in particular ways, a given technological device, system or protocol does not work. He goes on to say that this characterisation of security researchers is quite common within the broader field of computer science, often used in negative sense:

> *this is also why the IT security community are often criticised as these are the people that are destroying everything, or destroying everything without contributing much. It's justified to a certain degree, yes.* (ibid)

He also though points to the limits of such an analysis, arguing that focusing on the negative role of information security researchers ignores their more constructive contributions:

> *It plays an important role... and it's not always the case. There are new proposals for these distributed systems and stuff like that. So there are actually always a lot of new proposals that are out there* (ibid)

This indeed is a fair point, and by emphasising the critical aspects of the researchers work, undoubtedly certain aspects are lost. This decision though is justified both on theoretical and empirical grounds. In terms of theory, we have seen how critique has played such a central role within the frameworks of both Boltanski and Latour, and one of the central tasks emerging from this literature is an *agnostic empirical investigation of the various forms that critique can take.* With this thesis I want to contribute to this project by focusing on the critical activities of information security researchers. Moreover, empirically it was also found that while there were some positive elements to the researchers work, these were all at least preceded by some sort of critical move, and ultimately was engaged in far more regularly than other forms of research.

The critiques explored in this section will be arranged according to the researchers' different focuses in their work. Specifically, two of those I spoke two researched the security of the internet of things (IoT), three usable security and one blockchain. Arranging these in this fashion is aimed to clearly indicate how each of these research fields can be understood as a practice of critique. Furthermore the differences and similarities in these critical activities can be extrapolated, and will be the focus of a more analytical section that follows.

7.1.1.1 Usable security: (in)secure use of technologies

The work of *usability researchers* will first be conceptualised as a critical activity. These researchers are primarily concerned with understanding the role of the user within

information security and how the use of a technology changes its security requirements. Laura describes the field as:

> *my focus is on usable security and privacy which means we look at academic solutions for security and privacy which has to be a protocol or a scheme or whatever technical is there, and then we look at the intersection between this and the human.* (Interview 1, May 2019)

The researchers here generally look at how various users interact with and use different technologies and security protocols, focusing on the problems for information security that can arise with this. Within this, Laura focuses particularly on users' interaction with the Hypertext Transfer Protocol Secure (HTTPS), a central protocol for secure communication on the internet, Simon researches the use of blockchain technologies, and Julia hardware technologies.

Each of these usability researchers' work *critiqued the designers and developers of the different technologies and protocols* that they are focused on. They each argued that these developers have too narrow perspectives when designing digital systems´and, specifically, that they do not sufficiently consider user behaviour and its impact on its security. Laura describes this problem in the following quote:

> *Very often the protocols and algorithms work very well in theory but the application doesn't work because the people who designed it didn't think of the human who would use it at the end.* (ibid)

The aim of Laura's work is thus to better understand user interaction with particular security protocols, highlighting current shortcomings and recommending ways for these to function better. For one paper she looked at the HTTPS protocol "which is the protocol which you use when you surf on the internet." In relation to this there are two main groups of users: firstly, "end users, like for instance us when we are just surfing the internet." and secondly, "administrators who have to configure servers to use this protocol." (Interview 1, May 2019) Laura's research – an empirical study of how the HTTPS was understood and used by both these groups - found that for both of these there were problems with the protocol.

> *The end users really don't know what this protocol actually does and they believe that it does things that it does not and they don't believe the things that it does – which is encrypting all their information – they believe that it doesn't do that. So in the end why do we have it if people don't know what it does? And basically this thing with the administrators, we worked out why it is so poorly configured so often is because the configuration process is extremely complicated and even people who are extremely knowledgeable can't do it and make mistakes.* (ibid)

Thus Laura makes – *based on empirical research* – two specific critiques of the development of HTTPS. Firstly, that the purpose of the protocol was poorly communicated to end users, who then did not understand how the protocols, and, secondly, that it's proper implementation was overly complex, even for 'extremely knowledgeable' administrators, so that it often was poorly configured to the extent that attacks could still occur on a large number of websites.

She also explicitly underlines that her critique is focused on designers of the systems rather than the users. The mistakes and misunderstandings that she discovered highlights the failings of the design of the system, rather than failings on the part of the users.

> *the idea is that we definitely don't want smarter users, that users are smart actually that they just... I mean it is clear that you cannot know specific things, it also makes sense that you cannot know everything so we have to make, either we have to have a layer between the protocols and the users which makes the stuff for them, or we have to make the protocols simpler* (ibid)

Here we see an important feature of these critiques that will be repeatedly returned to: how they are directed at a particular group of people – the designers of the HTTPS protocol and related technologies – and that, at the same, they are the ones who are made responsible for enacting solutions to the problem. The implied solution to these problems with HTTPS does not come about through the education of users for example, but the better design of technological devices: "we have to make [...] a layer, or we have to make the protocols simpler" (ibid).

Simon gives another example of the critiques within usable security in his research on the use of blockchain technologies – distributed ledger technologies which are fundamental to digital currencies like bitcoin. He grounds his research in a broad negative assessment of overly technical focus in the development of IT systems.

> *I don't think you can separate IT systems and users and assuming that users need to interact with computer systems that they can interact with them so they of course like it and it looks nice and whatever that entails but also bad usability leads to mistakes that can have security implication and which then can compromise your privacy and things like that.* (Interview 5, June 2019)

He argues, similarly to Laura, that designers of technologies need to focus on the interaction between users and technologies, not the technologies in isolation, and that this focus should also include a security component, not just considering aesthetics relevant to users. His concrete work focuses on the use of 'wallet technologies', used to store the cryptocurrency bitcoin.

> *Here again we did a study on the users of blockchain technology with the focus on how they interact with the technology. So they have an interface which in that case is Wallet software and what are the problems with Wallet software - does badly designed Wallet software lead to loss of bitcoins, which is basically financial loss.* (ibid)

The critique here is very similar to Laura's – empirically investigating how users interact with a given technology and looking at the problems that arise from this use. Important here is that it is the designers of these technologies which are then subsequently critiqued; the loss of bitcoins indicates that a wallet software was "badly designed" - not, again, that it was poorly used.

Julia, also a usability researcher who focuses on hardware security, formulates a somewhat different critique from the previous two researchers. She argues that not considering the user in the development of a technology means that it cannot be used: "When you have a programme and you don't think about the user itself, you can have a technology or

a new RPE developed but if nobody can use it, it's useless" (Interview 3, May 2019). Elaborating on this Julia points to a technology's security failings as one of the ways that it can become 'useless':

> *"So the thing is – for example – the technology can just be adopted by the users, by the end users in this case, so if for example the users don't trust the technology because they don't feel safe, because they have read newspaper articles whatever, that something happened, they won't use this technology so it is useless in this case. As well, for example, if you are using your online banking system and you cannot trust it, or for example, it gets leaked then all your money is gone. Or you just don't use and still we all need our banking advice, so the automation is not used in a sensible way"* (ibid)

An important term here is *trust* – that users need to be able to trust a technology for it to be useful. The role of security researchers for Julia is to increase the trust in technology enough so that it can be used. Laura and Simon emphasise the need to consider users to make something secure, whereas Julia focuses on the need for something to be secure so that it can be used.

7.1.1.2 Internet of Things: hacks, honeypots and designing (in)security

Two other researchers - Markus and Lucas - focused on the Internet of Things, what Lucas described as "the initiative to connect everything" (Interview 4, May 2019). Research here relates to the increasing amount of devices connected to the internet, and the problems with information security that emerge with this. The researchers again each had different focuses within this: Markus's research looked at conventional or consumer IoT, while Lucas was concerned with Industrial IoT, related to increasingly autonomous factories, 'smart manufacturing' etc. The critical activities engaged in by the two researchers also differ in important ways.

Markus's work is generally based on a negative evaluation of the security features of newly developed devices that are being connected to the internet, and his research acts in various ways as a critique of this development. He is specifically critical of a the

manufacturers of these devices as the following quote indicates:

> *In this area of IoT the problem is a lot of devices are connected to the internet now which were never supposed to be on the internet and a lot of companies who have no idea about security because they are manufacturers doing devices and not security stuff, just attach a raspberry pie to this device and say "OK, now it is in the internet" but they do not think about the security concept. So you have a lot of devices on the internet now which are really badly protected and hackers or crackers are using this to exploit the systems* (Interview 2, May 2019)

He argues, in a similar way to the usability researchers, that a large amount of insecure devices are being produced and sold on the market because of the narrow focus of technological designers. Here, though, manufacturers are specifically positioned as the designers of technologies that are of concern. Furthermore their overly narrow focus is said to exclude consideration of security concerns altogether, rather than just the use of technology.

His research can be seen to be an academic practice of this general critique, which takes a form quite distinct from the other researchers. In general Markus makes the most use of *'hacking'* practices in the formulation of his critiques. One example of this is his hack of the smart watch that he was wearing during our interview.

> *For my PhD I hacked this watch, this smart watch from Huawei, because I wanted to have this watch and I received it on Christmas day and I invested the first two or three weeks twelve to sixteen hours a day reverse engineering it because the software for the mobile phone is really bad and I wanted to write my own software. Then I talked to our professor and he said maybe it is also interesting for SBA, maybe you can write a paper about it, so that is the stuff I am working on now.* (ibid)

Once again his critique is directed against those who designed the technology - Huawei - and it is their responsibility to make amends for this. Here, though, Markus critiques the watch by 'reverse engineering' it - "a process where an engineered artefact (such as a car, a jet engine, or a software program) is de-constructed in a way that reveals its innermost details, such as its design and architecture." (Leila, 2005, p. xxiv) The critical argument in his paper is that if

he can gain control of the device to write his own software, so too can a hacker and thus the device is deemed insecure. Interestingly he is also quite dismissive about the value of this particular form of critique "because to be honest its engineering, its reverse engineering, they are finding some flaw in the protocol that they implemented but its not a research where you say that this is something new and people benefit from some new methodology you can use." (Interview 2, May 2019) Here quite explicitly, and also more implicitly in the other interviews, engineering is contrasted with more 'scientific' forms of research, with the latter seen as more valuable, both by the researchers and also by conferences in the field.

He also describes his search for other topics to write his PhD thesis about - explaining that he would like to "analyze the firmware" - software strongly related to a device's more physical components "to find some security vulnerabilities" in different IoT devices. This is difficult, he says, because getting access to the firmware would be very costly. Markus's current solution is to develop a 'honeypot': a virtual replication of firmware that is used to attract and monitor the behaviour of hackers.

> *The idea of this research proposal is that we want to make a system that we can download some firmware from the internet so thirty, forty, fifty thousand firmwares and create a system which automatically starts all of these systems as honeypots and monitor what is going on.* (ibid)

This research is, strikingly, the least 'critical' in character of that described in all of the interviews. That is, it is not focused on the insecurities of a given technological system and the failures of its design. It instead provides an analysis of the various tactics of attackers and hackers. This research is also then in some ways closer to more traditional forms of security analysis (associated for instance with securitization theory), which focus on external threats rather than internal vulnerabilities. This helps to underline the specificity of critical character the rest of the research conducted at the centre. His work does also comprise a critical component by noting vulnerabilities within a device and which attacks are successful against this particular technology and its firmware, but it remains the most externally focused research engaged in by the interviewees.

Lucas, who researches the Industrial Internet of Things (IIoT), engages again in a quite distinct form of critical activity. In his work he focuses on the *historical* failures of

software developers and the presence of what he terms 'inherently insecure' systems in smart manufacturing plants. These inherently insecure systems are so-called because: "the only thing you have to do if you want to compromise or hack a system, you just have to read the manual." (Interview 4, May 2019) The existence of these insecure systems are explained by Lucas in a similar way as by other researchers – the designers of the systems did not sufficiently consider security when they were being built. He says:

> *The systems which we currently have are inherently insecure because security was not a big issue back then, forty years ago or that, and all these protocols, these network protocols we currently have, are inherently vulnerable because yeah they have not been designed with security in mind.* (ibid)

Here the past practices of developers are seen as problematic because this group did not consider security issues when designing the technologies. The flip side of this negativity is an understanding of the problem having improved in recent years, largely through the development of protocols that make security a fundamental part of the operation of these systems. He specifically cites the development of OCPUA - a protocol that, while focusing on other aspects such as communication efficiency, also includes security as a central component - as an example of positive change in developer practices.

This positive view of contemporary design practices leads to him critiquing the business who own and run these technologies, rather than current designers. He argues that these businesses need to replace their 'inherently insecure' systems with the well designed contemporary ones, and his critiques generally highlight the negative consequences of not doing so. One way he critiques these businesses – most similar to Markus's hacking - is penetration (or 'pen') testing, where a manufacturing plant is hacked and certain vulnerabilities identified.

> *In my past job I did penetration tests, so it was like a big steel manufacturer that we conducted a pen – penetration – tests emm and I was very impressed with this kind of task because we had to do some on site assessments where we really sat in this big plant and tried to hack the plant.* (ibid)

He describes this experience as a "flash" that helps to highlight that "if some security properties are compromised then really bad things can happen*",* giving the example of how an attacker could "steer a robotic arm in any direction and hit an operator" (ibid). Again the critical argument is that, if he as a researcher can successfully hack a plant, then so also could some more malevolent actor.

Lucas also, though, highlights the presence of more long term strategies of critiquing firms. In discussing the problem with manufacturing plants using already existing 'inherently insecure' technologies, he highlights how tackling this problem involves a lot of continual engagement with factory owners, engagement that struggles against the profit-driven logic that usually governs decision making processes in these factories.

> *When I visit manufacturing asset owners or the guys that run these big manufacturing plants, the operators and you talk to them about the security issues* [...] *'eh we don't want to invest in security because it always costs things and nothing ever happened'* [...] *And I mean this is a big issue because how can you convince management that there is an added value when you secure something? Which you cannot see immediately in terms of ROI* [Return on Investment]*?* (Interview 4, May 2019)

Specific forms of critique that Lucas refers to include highlighting the damage caused to other plants and using various tools to develop a probabilistic measure of potential financial damage.

Lucas's form of critique contrasts with the others, particularly usability researchers, in that here the contemporary designers of technology are not the subject of critique – he argues that new protocols being developed are sufficiently secure. Rather, he focuses on one particular set of users of technology: smart factory owners. While Laura, who focuses on usability issues, said that they "definitely do not want smarter users", this is exactly what Lucas is aimed towards: factory owners who better understand the security risks associated with their plants. This also relates to the overarching argument about these critiques delineating agency to those who they are directed towards – with Laura users are not positioned as responsible for their own security, while with Lucas factory owners are given the responsibility for making the changes deemed necessary.

7.1.1.3 Blockchain: empiricism and abstraction

The last researcher to be discussed is Sebastian, who focuses on blockchain technologies. He once again critiques the practices of the designers of particular technological systems and protocols, and argues that they need to increasingly focus on and improve the security of their designs. He specifically researched the Nakamoto consensus, which was the first paper produced that outlined the foundational protocols for the design of bitcoin and of blockchain technology in general. He describes his overall research as:

> *Over the course of my PhD I kind of recognised a lot of design issues with this original bitcoin protocol termed the Nakamoto consensus* [...] *It's a kind of interesting solution to an interesting problem but it has a lot of practical issues.* (Interview 6, October 2019)

This is quite a similar general argument to that given by the usability scholars: that the design of this particular protocol was overly theoretical, and it ignored the 'practical issues' that emerge as it is used. He elaborated on a number of distinct 'design issues' with the technology, often again based on the divergence between the theory and practice of this particular protocol. He argues that the original intent of the protocol was to create a "decentralized" system which was based on a notion of "one computer one vote". Instead of this, he argues:

> *it is actually not a decentralised system any more it is more like an oligopoly of Chinese miners, which has a pretty large influence in the system, so it is theoretically a very nice interesting protocol but practically it turned into an oligopoly of Chinese miners and this is of course not very desirable, from various reasons.* (ibid)

One of the papers he has published follows these concerns, and acts as a critique of how bitcoin actually functions.

> *so during my work we analysed also the internal structures of these pools and pointed out that even in these pools and even in these gatherings of miners there are also a lot large players in there,* [...] *there are even in these pools there are big players emm*

that contribute most of their computational resources obviously (ibid)

An interesting aspect to note here is the quite specific enactment of insecurity as an overly centralized structure of blockchain miners. Here the focus is on 'not very desirable' situations that go against the intent of the original protocols, rather than concerns around hacks or privacy. The form of critique offered here, though, is otherwise relatively similar to that given by the usable security researchers, empirically investigating the normal functioning of a technology, highlighting the undesirable aspects of this, to encourage changes in the design of these systems that will tackle these problems.

His work contains other critiques of the functioning of the Nakamoto protocol that highlight how it is 'fragile in practice' which take a different. One of these focuses on the *assumption* of honesty within the consensus, highlighting how this can be put in tension with another assumption of rationality.

> *You can create smart contracts that reward miners for dishonest behaviour if you basically pay them what you want them to do. And this is of course also a structural problem when you have a security or design problem when you have such systems, and so my thesis basically moved to this direction, what are the drawbacks of the newly proposed Nakamoto consensus and what are these issues, in that direction. and how can this be solved or can it even be solved or should design those systems differently?* (ibid)

This critique takes a more abstract form than many of the others. Here the argument is based upon theoretical inconsistencies of the predefined assumptions, with ideas from game theory and formal mathematics drawn upon. The critical force of the argument still remains similar - underlining particular undesirable outcomes of a technology that highlight the shortcomings of the design of a particular system. The application here is notable, though - that the problems of centralized control over a digital currency are rendered as a technical problem needing a technical solution.

Simon also points to an additional dimension of blockchain research in relation to firms – that at times they actively encourage the form of critiques offered by information security researchers: "There is a the C-CASH foundation which is the foundation behind this

kind of cryptocurrency and they have a lot of money and they started to give out C grants or something, and of course they only pay for research that basically improves their own system." (ibid) Markus describes a similar dynamic when referring to bug bounties – where critiquing a company's – for instance Google, taking Markus's example – software is encouraged by the offer of an award if a vulnerability is found. The general point being made here is the same – that the particular critiques offered by information security researchers can be seen to also be strengthening the position of those that are being critiqued. What this helps to outline is the specific form of critical activity that we are dealing with here: one that can be seen to strengthen the hand of those being critiqued, and is indeed sought after by these very actors.

7.1.2 Extra-institutional critiques

Apart from the researchers work itself being a critical practice, the researchers also engaged in other critical activities that were positioned explicitly outside of the discipline of information security research in different ways. There are two types of these critiques: firstly, those constructed by the researchers in their activities outside of academia and, secondly, those that were offered by them within the context of the interview itself. One of the main benefits of including these is that it helps in various ways to situate the critiques formulated by the researchers within institutionalized information security research. What is formulated in this context is thus seen to be only one part of the researchers' critical repertoire, which leads to questions about what can and cannot be included within the boundaries of this particular academic field and how the specific nature of the critiques gain their character. Also important are tensions between the institutional and extra-institutional critiques, pointing towards certain ambivalences within the study of information security for the researchers.

7.1.2.1 Critical hobbies

One way that non-institutional critiques emerge is through the work carried out by some of the researchers in their spare time outside of a formal academic setting. This includes certain practices of hacking, informal events, blogging and the construction of websites as a hobby.

Markus and Simon, in particular, see information security as a hobby that they

continue to pursue outside of their working lives, and construct a distinction between these activities and their normal research. Some of these activities are related to hacking, which Markus describes the basic idea of as "to use things other than they were meant to be used." (Interview 2, May 2019) In Markus's description of 'full' and 'responsible disclosure' we get a sense of some possible critiques related to hacking, and how these differ from those constructed within information security research. In both full and responsible disclosure hackers discover certain insecurities within a particular piece of software; with full disclosure, though, hackers communicate this weakness publicly by releasing the vulnerabilities discovered on to the internet, while with responsible disclosure they are first released to the company. In the interviews, Simon and Markus both made a point of saying that they had never 'fully' disclosed something, but had always given the information first to the relevant company. Markus explained the rationale behind responsibly disclosing something as follows:

> *The big problem is that large companies, particularly some years ago were not really interested in investing money into security. So they normally said 'yeah I don't care'. So the idea was to give the company some time, for example three months, I give you three months you have three months to fix it and then I will release it to everybody, because then they have the stress to fix it to release it otherwise its bad PR.* (Interview 2, May 2019)

In certain ways this form of critique is similar to research within information security, particularly Markus's own work, and other hacks that are used for research. Again with this critique we see with this how companies, through being the subject of the critique, are enacted as responsible for the provision of information security. The presence of the choice to fully disclose something here, though, indicates the possibility of this relationship shifting somewhat, with different, more confrontational relationships to these groups being constructed through a specific communication of a critique. Again, though, this form of critique was portrayed in a negative light by all the researchers who mentioned it.

Simon also described other work related to information security that he engages in outside of academia. He talked about communicating his research at informal meetups and his blog where he advises 'ordinary citizens' on potential ways to improve their security:

> *"I have a blog where I try to create or to talk about security em like easy ways to improve your security that usually is based on some kind of research or some things that I come across during my research"* (Interview 5, June 2019)

In this particular instance ordinary users of technology are the ones whose behaviour is problematised, through which they are delegated more responsibility for providing their own security. Here the design of a given technology is not directly challenged, but rather the behaviour of those using the technology. He also provided a rationale for engaging in this type of work, arguing that:

> *But at the same time having this communication to the general public which is usually the peers in your society which means your fellow citizens in the country, it is also important that they benefit from the research, because basically they also pay for it, but not only in terms of money, but I believe and maybe this makes me incredibly naive, I believe that we should progress as a human race. So why should only an elitist group progress and not everyone?* (ibid)

He here implies that research operating within the normal institutional boundaries of information security research is aimed towards an 'elitist' group - a focus which his blog allows him to act outside of. Concretely this primarily involves a change in who the (critical) communication is directed towards: in this instance he is focused directly on the behaviour of ordinary users, rather than on developers and businesses. This change in critical activity is understood as allowing these other groups to benefit from his work, supporting the earlier contention about the symbiotic relationship between critiques in information security and those being critiqued.

Lucas also gives an example of at least partially critical work that he engaged in outside of academia. His first project was a "privacy aware social network" which he positioned as a "competitor to Facebook" (Interview 4, May 2019). This experience is quite revealing and highlights certain tensions in the pursuit of privacy - and how these tensions can be productive for finding topics to research:

> *Emmm but of course if you track everything the visitor performs a reaction, the visitor performs on the website then this is very privacy invasive, you know? So really there is like this contradiction between the accuracy of this web analytics platform and the privacy features. So I tried to analyze how can I achieve a very good balance between accuracy - so tracking accuracy - and privacy.* (ibid)

Here again his work is based on an initial critical move - highlighting the empirical limitations of orthodox social media companies' privacy policies, as well as the more abstract tensions between the performance of a website through analytics and privacy. His work here, though, is more constructive and positive than much of the research conducted within academia by the interviewees. Here the critique led to an attempt to construct an alternative system to the currently existing ones, rather than arguing about how these can be improved. Here he makes himself primarily responsible for the provision of information security, at least within the confines of his websites. The relationship between the person that is being critiqued and the responsibility of providing security is here separated through the construction of a positive alternative to that which is being critiqued.

He also, though, points to the reasons for this project failing:

> *But of course it failed because I hadn't that big of an advertising budget, to recruit my users somehow. and social networks I mean they live from the users I mean if no one is engaging online then it kind of dies, it is a kinda graveyard, nothing gets published online, nobody will look into that.* (ibid)

Here we get a sense of the pragmatic and, in particular, economic constraints that guide the particular constructions of information security critiques. While this form of critique - with its attachment to a distinct alternative - appeared interesting to Lucas, if it also becomes a 'graveyard', then it has no impact on the actual provision of information security. This generally points to both the limits of, but also the necessity of institutional embedding of critiques - that only particular forms of critique can be articulated within these settings (often rather reformist in character), but these settings also offer the researchers an opportunity for their critiques to have any purchase on the external world.

7.1.2.2 Critiques within the interview

The last type critiques formulated by the researchers are those that emerged within the interviews themselves. Here the researchers often explored the broader implications of the work they were carrying out and certain processes that they are complicit with. Again here the notion of responsibility was important, with responsibility for these issues repeatedly delegated to social scientists.

One set of critiques that came up in the interviews were certain 'social' issues that were seen as an obstacle to effective information security provision. Julia for instance sees the inability of the different social worlds of information security to communicate as a central obstacle within the provision of information security - an obstacle that she saw as the responsibility of the social sciences to deal with.

> *These different worlds don't play together so well. And you can't just focus on one thing - it is already hard enough to get it technically right, so you cannot also focus on going to the standardization meeting and talking to all the different parties* [...] *so you guys have to find solutions for that* (Interview 1, May 2019)

Here a distinct division of labour between the social and technical sciences emerges - where the latter deal with the social problems, and the latter the technological ones - and as such the current work of information security does not itself need to be changed. The aim of the social sciences is thus a somewhat secondary one, focusing on the institutionalization of a relatively unproblematised notion of information security, pre-defined by the technical security researchers.

Another focus here was on the ethical implications of digitisation and technological development, with certain researchers offering broad critiques of these processes. Simon is particularly negative about the impact of technological developments, worrying that he sees "on a global scale technology progress outperforming human development" (Interview 5, June 2019). He also argues that this is a problem that cannot be tackled within the confines of information security, and instead this requires increased investment into the social sciences as a corrective. He says that "we need more humanity" within technical discipline and society more broadly, and that social sciences are the way to achieve that:

> *I also don't think you can distinguish the machine learning algorithm or see it as an isolated thing because it will always be employed in a context of humanity and I think more technically inclined people should get a worldview that encompasses humans, and for that we I think we need more social sciences.* (ibid)

The role of social science here is in some ways larger than what Laura imagined for it. While she claims that social sciences should have a more or less institutional role, helping to solve already defined problems around the efficient provision of information security, Simon sees them contributing a fundamentally different 'world view', with the orientation of information security research changing as a result.

Markus was perhaps the most elaborate in his critiques of technological development, and the relationship of this to information security research. He discussed how his experiences as a scout leader have led him to be concerned about the use of new technologies, particularly smartphones, among teenagers. He continued saying:

> *I think it is not possible to do basic research on each of these topics. And I think your area of research... When you say what impact has some new technology I think this is...? This is much more a topic for you than for us, because we can test if it works or if it doesn't work. But how it affects the world, some new technologies, which impact it has, and yeah, how it changed the world for me it's really important* (Interview 2, May 2019)

Here the limits of the discipline of information security are explicitly drawn: that the value of technological development is not questioned within information security research and largely taken for granted. Researchers in information security have only the narrow focus of whether 'it works or if it doesn't work', rather than questions about the value of technologies and their impacts. Also notable is how the critiques that he points towards here - the sometimes negative impacts of technology on society – are again delegated to social scientists. Here the social scientist is given responsibility for dealing with fundamental normative questions about the development of technology and its impact on humanity. Like with Laura a division of labour is constructed between technical and social scientists. Here though, the social

questions are positioned as fundamental – as that which can challenge technological development and what security within this can mean.

All of these critiques help to point to the specificity of the critical activity found within academic information security. Primarily, this is in relation to the subject of the critique. Within almost all of the academic research outlined by the interviewees, the subject of critiques were the designers or owners of new technologies, and these actors were, through the process of the critique, made responsible for information security in this particular domain. Outside of the SBA this relation differed though – with hackers, users, information security researchers and social scientists, variously made responsible for the problems related with information security. We also saw how in certain instances the problems themselves broadened beyond whether, in Markus's terms, the technology 'works or not', but to concerns about technological development in general and how this is changing the world. The rest of this findings will explore the conditions of the emergence of the particular critical activity found within information security research. It specifically will looking at this specificity as related to two sets of value practices: the researchers' own ones (justifications) and institutional ones (tests).

7.2 Justifications

In this section I will outline some of the justifications the interviewees offered for their work. Having examined the 'critical' content of the research in the previous section, stressing particularly the specificity of this content, this section will move on to address the value practices that this particular content is emergent from. Specifically, this section will address the justifications that the researchers offer for their own work; that is, the particular value that they attribute to their research. These justifications will be delineated by the central actor or process that the research is said to benefit from the research. Three general registers within which the research was attributed value were determined in the analysis: protecting users of technology from harm, engendering trust in the process of innovation and fulfilling the researchers' own personal demands.

7.2.1 Protecting the user from harm

One of the central ways that the researchers justify their work is by pointing to the benefits that accrue *to users* of technologies with more secure digital systems, and the dangers to these

individuals of insecure systems. As Julia put it:

> *In our research field at least we want to strengthen the whole security and privacy aspects for all end users never mind if they are European, Asian or African or American. or, I don't know, Indo-China or whatever* [...] *it is all about the human factor.* (Interview 3, May 2019)

This perspective - where a generic human is put forward as that which the researchers aim to protect - was a common form of justification for the research throughout the interviews. The type of harm being discussed, though, as well as the users being effected, changed throughout the different interviews

This harm that could directly affect end users was most often presented in terms of *privacy* implications. One common theme in the researcher's focus on privacy was that it acted as an initial inspiration for the researchers' career in information security, and acts as a justification for the overall discipline. Laura, for instance, was explicitly motivated by privacy issues, saying that she was in general concerned about "so many companies collecting our data like people becoming completely transparent and so on and being spied on and these things." (Interview 1, May 2019). Similarly Simon states that he was also interested in privacy for a long time: "Privacy I was already very interested before because... I don't know why to be honest but I was always fond of privacy and being able to keep things private." (Interview 5, June 2019) This was also an initial motivation for Lucas, whose first project was a "privacy aware social network" which he positioned as a "competitor to Facebook" (Interview 4, May 2019). In each of these examples privacy is positioned as valuable in and of itself, and the researchers do not generally elaborate on why they view privacy as so important, nor do they connect it directly with their current research.

Some interviewees did though justify their current research interests on the grounds that it led to increasing privacy for end users. Simon, for instance, talks about the benefits of cryptography in these terms.

> *we have to employ encryption or cryptography to ensure things in the digital space that we could do in the analog space we could go into your living room which is sufficiently private but on the internet basically everything is public. But in order to*

create these private spaces we need cryptography. (Interview 5, June 2019)

Here privacy is positioned as something that is normally attainable within the "analog" world, but that is difficult within the digital space - so he understands his role as helping to construct these private spaces. Here privacy is in itself positioned as desirable, something that we do and should expect in our communications. The actors that the privacy is protecting users from here is, though, left somewhat vague. Laura also justifies her research in terms of providing privacy for end users, and she provides a more concrete example of how this is materialised. Her work is based around the HTTPS protocol, which she explains in the following quote:

> *This protocol is basically the protocol that gives us the security that if we communicate with another website that nobody in the middle can read our stuff. If this is a password or a bank transaction this is of course important that it really does stay confidential, especially if it is sensitive information* (Interview 1, May 2019)

In this example the worth of privacy is tied to other forms of harm to justify its worth, rather than seeing it as in itself valuable, i.e. it results in fraud or financial loss. This quote is also notable as it highlights how *privacy attains a specific character* in her work and points to the different meanings that privacy can have within different research projects. In Laura's research privacy specifically protects users from unauthorized access to their information by third party 'attackers', and does not protect against the tracking and gathering of data by the 'endpoint' company.

> *The protocol is just about encrypting the information between you and lets say Facebook. But for the thing that Facebook who is the endpoint who is everything unencrypted of course can collect your data that is a completely different thing.* (ibid)

While her initial motivation was concerns about "so many companies collecting our data" and the implications of this for people's privacy, her research, while still justified according to privacy, does not tackle these issues.

While Lucas understood that privacy was a large concern in a number of fields ("with E-Health applications it is of course a very big issue, also with smart cars, smart homes and

so on*"*), he also argued that in his particular line of research (Industrial IoT) it is not a priority. He says that researchers here are "not really [interested] in preserving the privacy of your employees or your factory workers or something like that.*"* Lucas still, though, justifies his research in relation to the potential harm that may happen to individual users - but he instead emphasises concerns about 'safety' rather than 'privacy'. He describes these concerns as:

> *Because the production systems of course they interact with the raw materials and produce goods and so on and if em if a hacker is able to compromise these systems and maybe I don't know and steer a robotic arm in any direction and hit an operator or something like that, this has direct safety implications. and could even harm human health.* (Interview 4, May 2019)

While this is less of a concern for the other researchers, Simon also justifies his general interest in security in relation to potential physical harm caused - pointing to how in automated driving and other applications "I put my life in the technology*"* and thus increasingly depend on these systems being secure from external attacks.

The different types of harm that can be done to the users of technology is also seen in the changing understanding of the value of blockchain technology and research into this field. According to Sebastian, it was first thought that blockchain could provide useful security functions because it was a "privacy preserving technology". The credibility of these claims, though, were quickly undermined:

> *The first publication looked into the claim that it is anonymous and said ok there are certain drawbacks, it was quickly found out that it is not that anonymous and not that... and yeah all these privacy and anonymity claims did not really hold to that extent* (Interview 6, October 2019)

Rather Sebastian justifies his research on the grounds that blockchain "is a very transparent system", a transparency which lends the technology a number of useful applications. Subsequent research focused less, then, on the security potentials of the blockchain system, but in attempting to secure *its* application as a cryptocurrency.

> *Because there were also money involved and people were holding quite substantial amounts of it, they also had a large interest in securing their funds. So a lot of start-ups were created actually to be dedicated to how to secure funds* (ibid)

Here again the users of the technology are positioned as needing support, but this time it is in order to *secure* their financial funds that is the main thing being protected, rather than any valuing of their *privacy* per se. An interesting dynamic here - and more implicitly throughout the interviews - is the relationship between the central terms privacy and security. While these terms are very often used together - and occasionally interchangeably - they are not synonymous with each other. One important shift is that within a discourse around privacy, large companies can be positioned as threatening, while this is not the case within a notion of security. The various uses of these terms across the broader field of information security research would be an important area of further research.

7.2.2 Engendering trust in innovation

A second set of justifications which the researchers offer for their work is related to the benefits that the work will have for the process of innovation in general. Here the researchers base the value of their work on contributing to the technological development of contemporary societies, particularly processes of digitisation. They specifically argue that there is a need for these systems to be secured (through research), in order for them to be trusted by society, and thus for their implementation to be a success.

This register of justification was articulated particularly clearly by researchers in the usability sub-field. Julia, for instance, says that one indication of bad usability is if a given technology is not adopted by users because they do not trust it. She puts it the following way: "if for example the users don't trust the technology because they don't feel safe, because they have read newspaper articles whatever, that something happened, they won't use this technology so it is useless in this case." (Interview 3, May 2019) The key term in this sentence, and is this overall register of justification, is *trust*: the researchers' role here is to increase users' trust in a given technology. In this line of thinking her job becomes to make sure that the users 'feel safe to use the technology' to the extent that it is actually adopted by the users.

Lucas justifies his work in this light, as supporting and securing the process of digitalisation. In general terms he frames his research within an environment where "connectivity always increases, we are always trying to transform businesses and transform our government digitally.*"* (Interview 4, May 2019) He grounds this in relation to his field of Industrial Internet of things and "the strategic initiative industry 4.0 which means we connect everything and we need to make the systems interoperable" (ibid). Within this Lucas then justifies his work for helping the continuation and growth of these processes of digitisation and innovation. He looks specifically at the German government's plans for industry 4.0 saying that

> *Yeah I think in general the cyber-physical systems domain is also the future, in particular the strategic plans of governments or organizational bodies because for example with the industry 4.0 it was just Germany's plan to establish an interconnected smart ecosystem of factories.*[...] *And if you really want to succeed in doing this or implementing these strategic initiatives or plans to get ahead then we have to treat security as a first class citizen and establish security up front because otherwise these plans are designed to fail.* (ibid)

Information security is here positioned as securing initiatives like that being developed by the German state and thus the digitalisation of contemporary economies and societies. If security is not sufficiently focused upon in these developments they will be insecure and suffer attacks, and they will be unsuccessful. Important to underline here is the role of companies and governments within Lucas's justification of his research - here they are positioned as the actors whose interests are being secured. Rather than being that which is seen as threatening, as in certain registers, it is their innovation plans and profit margins that are of central concern here.

A similar logic is also employed to justify research into blockchain technologies. As we saw research in this area switched from seeing the technology in and of itself as a security enhancing technology, to being a technology that was being widely used but was insecure in many ways, and thus research into the area was needed to further this security. Further to this, research into the area was justified by Sebastian as being necessary for the continuing successful development of blockchain technologies, particularly in relation to their

application in the cryptocurrency bitcoin.

> *that's the answer what security... what is the connection to IT security? Of course if you have money involved you and IT systems you want a good IT security because otherwise it will not work as a whole. If you cannot trust in your IT systems and trust in your interaction with these systems you will not trust in a digital money system if you cannot trust in the security of a digital IT infrastructure.* (Interview 6, October 2019)

Again the researchers' role in this register is not primarily to protect users from harm, but to make them *trust* the technology enough for it to be adopted by them. While most of the researchers did not expand upon why they felt that these new technological developments should be supported, Sebastian's support for the development of blockchain technologies was explicit and grounded in a clear rationale: "it is a method of decentralising stuff". He refers to the internet initially being "very decentralised" with "a lot of players". He argues that this has changed and that:

> *during its lifetime it got more and more centralised and basically the underlying architecture of the internet there are a small number of big backbones and groups so it got more and more centralized.* (ibid)

The internet is now, he says, dominated by "Facebook and Google and Twitter, these huge sites. Against this, blockchain technologies promise to:

> *allow a certain degree of decentralization again so you can distribute trust amongst a set of participants you can choose emm and if the majority of them acts honestly then you can agree or decide on a result that is valid and you can possibly trust in a single participant.* (ibid)

Sebastian constructs his research as being valuable as it contributes to the development of blockchain technologies, which in turn contributes to a broad process of decentralization. In this specific framing large tech companies are again positioned as being threatening to the

desirable state that he is trying to secure - highlighting again their ambivalent position within this register of valuation and, potentially, in the overall discipline. This register of valuation also has an ambivalent relationship with some of the critiques raised by the researchers in the interviews. As we have seen, Markus and Simon, in particular, pointed to the negative effects of technological innovation. Markus voiced concerns about these trends - both for their impact on information security and on society in general - but he said that questioning these trends is not a topic for information security researchers and that they are largely taken for granted in the field - "because we can test if it works or doesn't work". Here we see certain ways in which research in information security is connected to and supports the trends that Simon and Markus present extra-institutional concerns about.

7.2.3 The researchers' self interest

The final justification presented by the researchers for their work is concerned primarily with the career and lives of the researchers themselves. In this register the aims of their research are not outward looking, but are positioned to be in some way to serve their individual interests. Two themes emerge within this broad register - firstly their progression within the field of information security and beyond, and, secondly, their personal enjoyment of their work.

Many of the interviewees expressed a desire to progress with their career in information security - and justified the worth of their work in relation to the potential benefits it has for this. When Laura, for instance, was asked about whether her previous project was a success, she answered in the affirmative because:

> *I personally learned a lot. Because I got my first publication at an A* conference, I am one step closer to my PhD. and this is actually the main thing that I think it is successful* (Interview 1, May 2019)

The main justification for the research here is not on the impact of the research on the general provision of information security, as with the other two registers, but on its impact on Laura's professional life. A valuable piece of research is one that brings her further on the path to securing a PhD. This highlights how the value of the research is defined in part by the institutions within which the researchers are embedded. This sentiment is shared by many of

the PhD students, who regularly cite the need to prioritise work that will allow them to finish their PhD as a priority when researching. Researchers in blockchain, for instance, cited the 'hyped' nature of their chosen field of study as a rationale for exploring it. Simon is most explicit about this:

> *I guess I also fall in the trap again that I am looking at a very sexy topic but I'm a child of my time so of course I look at the things that are interesting right now* (Interview 5, June 2019)

This valuation practice is also possibly more important for my interviewees particularly at this stage of their careers - all of whom are PhD students - and are more focused on progressing through the field rather than immediately making a material impact within the provision of information security. Markus for instance talked about how he is too young to really make an impact on the broader provision of information security, while Simon hopes that he can have such an impact but has a timeline of thirty to forty years in mind. Although he sees this lack of broader impact as a "sad topic", he is still happy on a "personal level" to pursue his research and write papers as a way to communicate his findings and develop as a researcher. On a "professional level" as part of his PhD he is required to publish papers at conferences and the character of his research is constrained by pragmatic concerns about achieving this particular end.

Lucas has a slightly different set of concerns than the others in this regard. For him his professional focus is predominantly on returning to the industry, and he is in part pursuing his PhD research as a tool that will 'open doors' for him in this pursuit. This particular personal focus has an impact on the work that Lucas engages in within his PhD:

> *after my PhD I also have plans to get back to the industry and not pursue an academic career so I'm more interested in the applied stuff. I'm involved also a little bit with the consulting group of SBA and yeah I'm not not 100% researching but also, you know, doing some qualification workshops with company partners that SBA organises. So like giving lectures and so on. But most of the time I am doing research yeah, and I'm trying to get my PhD done and yeah.* (Interview 4, May 2019)

The work that Lucas engages has a more 'practical focus' than the other researchers - focused on engagements with industry - a focus which is justified because of the value it will hold for later employers and his career progression through the industry. What this again emphasises is the relationship between the researchers' valuations and those of the institutional environment they are situated within. The researchers here are not autonomous agents who live in isolation - or are in command of - a broader social context. Rather their research and processes of valuation are constrained by institutionalised orderings of value. An exploration of the effects of this institutional context is thus needed to get a sense of the emergence of research focuses within the research centre.

While many of the researchers, then, justify the worth of their research in relation to personal benefits, these benefits are not purely based on career progression but also the general enjoyment that they take from the research. This logic is most explicitly referred to by Markus, who sees his PhD as a way to balance working and having a hobby at the same time, claiming that the primary rationale behind his topic choice is enjoyment: "I just want to have fun to be honest" (Interview 2, May 2019). This is particularly relevant as Markus first became interested in security as a hacker and at first he says "I was only happy about doing my stuff, I can hack things, and I can search my project I am interested in and do this." (ibid) Though the longer he has spent time within the research community, the broader value of this work has become increasingly important.

Simon also became interested in computing because of a personal interest in graphic design. While his pursuit of this is now generally outside of work, he still finds his research to be a good creative outlet: "I find this a very creative process and a very creative approach to very abstract system and that makes me feel good I think." (Interview 6, October 2019) Julia also explicitly references her personal enjoyment doing research, saying "I really love to do the things which I am interested in and investigate it further." and she describes collaborating with her colleagues as: "we are often sitting together and brainstorming together with new ideas and all the creativity comes together and it blossoms, kind of, and I really enjoy it." (Interview 3, October 2019) Here we see how two quite distinct forms of self-interest operate within the research centre: the first focused largely on career progression within or outside of information security research, the second focused on personal enjoyment of research through creativity, collaboration and experimentation.

In general the justifications offered by the researchers point to the *multiplicity of*

moral orders present within SBA Research. Here we see how the emergence of research concerns within the research centre is a complex phenomenon, justified according to three relatively distinct notions of value. The researchers are thus here seen to be active and reflective within their research – with many of them offering different justifications for the same piece of work. They sometimes justify research, because it is fun, or that it helps protect an actor from a particular piece of harm, or for its contribution to economic and technological development. Thus one way that the researchers interests can be seen to emerge is through a process of *balancing* these different notions of value, pursuing work that can be simultaneously justified according to these different notions of value.

7.3 Value orderings and tests

This section will look at the institutional environments that the researchers work within. The primary aim with this is to understand the role these have on the emergence of issues of security concern within information security research. I will begin by addressing the level of the researchers immediate working environment – SBA Research - with an interest in the orderings of valuations found here. David Stark (2000) uses the notions of heterarchy and hierarchy to examine the ways that valuations are institutionally arranged - the former referring to situations with multiple legitimate forms of valuation, and the latter where one particular form of valuation is dominant. The orderings within SBA are generally presented favourably, as a rather heterarchical ordering of value, particularly in contrast to accounts of work within the 'industry' of information security. It will be underlined, though, that while the researchers emphasise the relative openness of the environment within SBA Research, certain valuation practices do remain (implicitly) dominant and constraints on research persist.

This will be followed by an account of the two main tests that the researchers' work is subject to: 1) getting funding for their PhDs and 2) getting papers accepted at conferences. Underlined here will be the different ways that these tests impact on the research conducted as well as the ways they are contested within the interview, specifically looking at how the researchers present conferences as the more legitimate evaluation.

7.3.1 Working in SBA – Relative heterarchy

This section will outline the accounts of SBA Research provided in the research, relating

these to notions of more hierarchical or heterarchical orderings of value practices. In general the researchers present the working conditions in SBA research in a positive light, emphasising how they find it a good environment for conducting research. One important reason for this according to the interviewees is the openness of the centre and the freedom that workers experience there. Julia emphasises this in the following:

> *Researching here is so open and you discover so many things [...] here it is more like open and you are allowed to discover certain things and research about it and because of this freedom it is, at least it inspires us, like in our group* (Interview 3, May 2019)

This quote highlights the underlying argument of this section - that the researchers present SBA Research as having a rather heterarchical ordering of value. The researchers have the freedom to work on whatever project they want because various valuation practices are considered legitimate and, indeed, necessary for research. Markus, for example, states that "when someone at SBA research has an idea, let's do that, it is not a big deal to say lets try it and see if it works." (Interview 2, May 2019) He goes on to outline his process of researching in SBA:

> *I can search a topic which I am interested in, I can teach myself the basics.*[...] *so I can get into this topic and then I can do it for three months, six months, however long it takes and if I have enough of it, hopefully I finish it with a good paper but then I can search for the next topic.* (idid)

The researchers generally position themselves as having a good deal of autonomy within SBA - they are allowed to pursue their own interests without much immediate intervention from those more senior within the company. Indeed some of the interviewees expressed difficulties with adjusting to the freedom that working in SBA offered. Laura provides one example of this, when she described the difficulty in her transitioning from her previous studies:

> *And when I started here it was like 'do whatever you want, whatever you can publish*

> *at the top conferences. just do it!' and then I was like oh my god I have no idea what I should do, actually, so there was no guidance at all.*(Interview 1, May 2019)

While Laura describes this initial difficulty with the openness of what is considered potentially valuable research at SBA, she, like the other researchers, still offers a broadly positive assessment of the working conditions there.

In general this favourable assessment of working in SBA was based upon an overall preference for academic research in general. One way this was expressed was through comparisons between 'research' and 'the industry', where, generally, work in security the industry was associated with more constraints on research practices, and only particular forms of research are immediately considered valuable. Julia, for instance, says that why she finds research so attractive is that "There are so many other jobs where you are forced to do something" (Interview 3, May 2019)**,** where a particular organizational value is dominant. Markus, who spent a lot of time working in security consulting, was particularly strong on this point. He focused on the temporal pressure experienced when working in consulting - where in research he had several months to explore a topic he was interested in, in consulting "you have a project for one or two weeks and your job is to destroy things and find something [...] so you always have the stress to find some vulnerabilities, find something new, and there were a lot of projects that didn't make sense in my opinion*."* (Interview 2, May 2019) Comparing his experience in consulting in the industry with the work of SBA's consulting group, which he sees in a more positive light, he says the latter can perform their job better because the "get the time to do things"

What accounts for these very different regimes? Markus argues that it has a lot to do with the economic organization of SBA - and the absence of profit as an organizing register of valuation.

> *SBA research is a GGMBH so it is a special form of company, the company does not take, or the owners do not take the money at the end of the year, they are not allowed to do that. They can only leave it in the company and reinvest it.* [...] *So they are not that interested that the company gets bigger and bigger and performs better. And so there is not this stress.* (ibid)

Laura also agrees with this criticism of the profit oriented nature of industrial information security, in her case discussing her experience working for two years within a standardization agency. She describes a "clash between these two worlds" of standardization and research, where the former "don't aim at research and they don't always aim for things to be correct - it is the end a lot about money and politics as well, unfortunately." (Interview 1, May 2019) Elaborating on this, she says that "all the companies want to have their solutions in the standard, they don't want that to be changed, they don't care about having additional work because some researcher says yeah but actually this is not secure," (ibid) This also underlines the fact that SBA is not only an enjoyable place to work because of its openness, but that this institutional structure also allows for better security outcomes, as defined by the researchers.

While, then, it is clear that the researchers position SBA as a particularly open security institution, where researchers are free to pursue their own interests according to their own logic of justification, it is also not, unsurprisingly, a perfectly heterarchical institution. Rather the researchers highlight that the institutional value of their work is largely defined in relation to two specific tests - its ability to attain sufficient funding, and its acceptance to highly ranked conferences. While this will be explored in detail in the following section it is important to briefly note its importance for the organizational dynamic here. Returning to a quote from Laura above she characterises the working environment within SBA as: *"'*do whatever you want, whatever you can publish at the top conferences. just do it!*'"* (Interview 1, May 2019) She says further that

> *Well yeah actually for us it's like this that we don't have to work on one specific topic like for all the years you can be a little bit more flexible you can work at whatever can be published at the top conferences in our field so I did a little bit of different things* (ibid)

While the researchers are free to explore whatever topic appears interesting to them, based on whatever rationale, this rationale must ultimately agree with the logic of the 'top' conferences where the researchers must publish their work. Indeed, while it was noted earlier that the firm offers little specific guidance for coming up with topics to research, it does offer a good deal of institutional support for dealing with issues around funding and conferences.

> *Yeah but we are really lucky here at SBA because we have two or three people who help us with all the organizational stuff and all the paperwork and so on. We are really just responsible for the content* [...] *we have quite a good wheel of process when we are thinking about the proposals.* (Interview 3, May 2019)

What this, first and foremost, helps to underline, is the predominance of external institutional constraints on the researchers, as opposed to the internal checks from within SBA Research itself. It also points to the limits of conceptualisations of orderings of valuations under categories of hierarchy or heterarchy within this case. Even in this situation, which to those working there is characterised by a regime of great flexibility and freedom, specific dominant tests of worth still persist. While situations may be more or less hierarchical in their orderings of valuations, it appears unwise to ignore the, perhaps indirect, constraints that operate on actors in situations of perceived heterarchy. The last section will explore the concrete tests that arrange work conducted in SBA Research, and, to some, extent, information security more generally.

7.3.2 Institutional tests of value

The last point of the findings will be based on the concept of *tests.* For Boltanski (2011, p. 50-82) tests are the central way that principles of worth are ordered and made concrete through which various powerful actors from the social world in some specific way. This section will explore two specific tests that repeatedly emerged as prominent within the findings: attaining funding and being accepted to conferences. As Sebastian puts it, "these are the two major things. Without funding you cannot work and publish at conferences and without publishing at conferences you will not finish your PhD." These tests will be discussed in relation to the main form of value that they perform, as well as the ways that the conferences themselves are evaluated and contested. In general it was found that conferences, which perform a notion of value centred around 'scientific worth' were seen as more legitimate than funding, which was associated with a more economic notion of value.

Before describing both of these tests in turn, a quick note on the reduction that the analysis is based on here is important. That is, while focusing on these two tests is a reasonable simplification it also excludes and makes invisible certain other forms of work involved with pursuing a PhD at SBA Research, and other ways that the value of the

researchers is determined. Sebastian, for instance, is partially critical of such a reduction and points to the undervalued work that these two tests ignore:

> *Usually it should not be only those two things, and what I actually like during my phd, is teaching which not all phd students like because again it costs you a lot of time* [...] *but again this is something that is kind of assumed sometimes but is not honoured* (Interview 6, October 2019)

Thus, one risk in my argumentation here is to make parts of the PhD that are already undervalued further invisible, and it is important to keep in mind the variety of work undertaken by the interviewees within and outside SBA and numerous (more or less formalised) mechanisms for ordering their worth. Nevertheless, conferences and funding were repeatedly referred to as the two main ways that the value of the researchers work was *institutionally determined* and thus will be the focus of this section.

7.3.2.1 Conferences

The first set of tests to be explored are those of being accepted to present papers at information security conferences. In this section I will outline the central valuation enacted by this test - 'scientific worth' - and the generally positive assessment that the interviewees offer of it.

Publishing papers at these was presented in all of the interviews as an important way that the value of their research was established. The prominence of conferences is quite a distinct feature of IT security, something that Sebastian puts down to the fact that "publishing cycles are very fast" in this discipline. These conferences are also themselves ranked - with four conferences being the highest with an A* certification - and all of the researchers talked about the need to publish at highly ranked conferences. For instance Laura says: "We are required in order to finish the PhD to have a certain number of papers at conferences above a certain level." (Laura). In general the type of value that is enacted by these tests is said to be 'scientific worth', an ascription that was regularly referred to in the interviews, though with little empirical content. For instance, both Laura and Sebastian favourably compare conferences with, respectively, standardization and funding agencies. They both argue that the latter are characterized by a focus on economic value whereas conferences are considered

with ‘scientific value’ (Sebastian, Interview 6, October 2019) or ‘research’ (Laura, Interview 1, May 2019) but no further detail was provided on this topic. One exception to that is in Markus’s discussion of why he thinks that his project (hacking his watch) is not sufficiently interesting for a highly ranked conference.

> *Because to be honest it’s engineering, it’s reverse engineering, they are finding some flaw in the protocol that they implemented. But it’s not a research where you say that this is something new and people benefit from some new methodology you can use.*

Here interestingly the critical character of the research that was earlier described (or at least some form of it) is portrayed negatively, and that valuable scientific research is comprised of more positive components. Other than this, though, the notion of ‘scientific value’ was left rather under explored within the interviews.

In general conferences were usually portrayed in quite a positive light - as a central aspect of conducting research that fulfils many useful functions for the researchers. One aspect to this is that they are portrayed as being the means through which the research can be communicated and, ultimately, make some sort of impact. This is specifically how Simon assesses their worth: “communicating science is part of research otherwise I think we fail so that is where I would put the conference thing.” (Interview 5, June 2019) Failure here being the inability to put research into practice. Laura similarly sees publishing conferences as important (if imperfect) fora for communication between standards agencies, industry and research. It is through this communication that standards can later be implemented and practices changed, saying: *“*if you just do your research and have some perfect protocol, if you don't publish it and if you don’t get it to any standard nobody will use it*”* (Interview 1, May 2019)

The communication that is engaged in at the conference is also two-way and some of the interviewees talked about the value in attending presentations given by other research groups. Julia, for example, describes attending one conference:

> *“yeah it was very interesting to see all those different people from those different research fields and there were pretty well known names as well, like for example from the Diffie-Hellman algorithm, one of the main authors was there and presented his*

work and it was kind of "wow that's our hero there". (Interview 3, May 2019)

Simon sees this in a similar way, viewing conferences as an important way to get a sense of the current sets of priorities within the information security field, as well as becoming embedded within the broader community. "I mean personally I would say I think it is interesting to get a picture of what the other people are working on and also networking [...] it is nice to talk with people and have faces to the papers you usually only read online*."* (Interview 5, June 2019)

Another related function of conferences is that they act to validate the work of the researchers. Important in this is that the conferences are ranked against each other, with four conferences in information security given the top A* ranking. The researchers are not only required to publish, but also to publish at a number of highly ranked conferences, so the work that these specific conferences deem worthy of publishing becomes important. Laura is here most direct, saying that she sees her work as successful because it was accepted into a top conference - *"*I think if the people at the A star conference liked it then it has to be good*."* (Interview 1, May 2019) She further elaborates on why this is, highlighting the senior position within the community of those responsible.

> *And they all have programme chairs, and they get the top people in the different fields for reviewing the different papers. So for instance if I now submit a paper and I say it's in a usable security area, then all the people in the programme chair who are in this area will review my paper. So this is the idea that the top people in their area, they review your paper and* [...] *if you get it accepted by the programme chair, then it should be good. because they are the top people in their area.* (ibid)

Markus provides a complimentary counter-example to Laura, in that he argues the inverse - while his current work is interesting to him, he is quite sure that it is not worthy of being accepted by the top conferences. At first he argues that this is due to certain technical limits of the research - "it is only engineering" (Interview 2, May 2019) - but he then points to the incompleteness of this diagnosis - there are engineering projects accepted by top ranking conferences because they impact a large group of people, using his example. This points to the various registers of valuation utilised within these tests, undoubtedly an interesting topic

but unfortunately beyond the scope of this particular study.

In the following quote we see how these two logics of validation and impact can also work together - by being validated at conferences, the work gains credibility and is more likely to make an impact. Laura states that:

> *The thing is also if you publish a paper at an A* conference, it has a much wider popularity tend to look at it, because it is more serious and it has a really well known name and also the peer reviewing process is kind of strict and hard, so the people know it has to be a good quality. And I think everyone in our firm wants to have an impact and change the world to a better place, lets say, so of course we want to publish at the A* conferences.* (Interview 1, May 2019)

What is most important to underline from this - and what a lot of what was previously written ultimately amounts to - is that it is conferences, and the test of being accepted by these, that are particularly influential in terms of the emergence of research focuses. Julia gives a particularly detailed description of this process in her account of how she came to focus on her current topic. She began by exploring a particular interest and then seeing that there was no work in this area but that:

> *there were several keynote speakers from the last two to three years* [talking about the topic]. *Okay if some people are talking about it and no research has been done yet, so it must have been urgent, because otherwise the people wouldn't have been talking about it.* (Interview 3, May 2019)

Conferences, and keynote speeches in particular, act to validate particular research interests defining what information security research is considered to be worthwhile. Simon gives a similar view of how embedded his focuses are within the priorities developed from conferences, particularly by looking at the correspondence of his research to various 'hype cycles'.

> *I mean when you are at the conferences and you see that the topics at the conferences and we have this ranking of conferences that we ought to try send papers to, and they*

> *for example change* [...] *and recently many or basically all of the big conferences also included blockchain technology.* (Interview 5, June 2019)

Both of his research topics he admits have been 'sexy' topics, something he reasons in the following: "I guess I also fall in the trap again that I am looking at a very sexy topic but I'm a child of my time so of course I look at the things that are interesting right now*"* (ibid). Here the phrase 'child of my time' is notable - while Simon has researched topics that are in vogue, the relation here is not a direct one where conferences directly determine what types of research are considered are valuable. Rather the influence is more intangible and amorphous, with conferences also presumably being children of this particular time, and not directly responsible for the emergence of this research concern.

Blockchain research presents a further qualification to this, and its relationship with these tests points to ways that the notions of value enacted by conferences can also be challenged by research practices. As Sebastian explained, blockchain began as a marginal area of study which was "just published on a mailing list dedicated to more crypto people or crypto-anarchist people" and it "did not have its own publishing community in the academic world" (Interview 6, October 2019). It later experienced a period of growth and became a particularly prominent topic within the discipline. Sebastian argues that this was in part due to the fact:

> *it was 2009, it was this time where big bailouts from the banks came, they were not very happy with the current banking system, so it rided on this underdog image there is a new cryptocurrency, totally backed by technology and cryptography, you don't need to trust anybody.* (ibid)

Again we see here how the interests of both the PhD students and the conferences are further shaped by very broad historical events and macro sociological processes. While this is of course beyond the scope of this thesis, it also helps to complicate any simple causal narrative about the emergence of research concerns within information security.

While, then, conferences appear as relatively important sites for the emergence of research concerns, this function is also largely uncontested. These tests are in general not subject to the same level of criticism as funding agencies, though certain criticisms do

emerge. As we have seen, Markus pointed to certain ambiguities within the frameworks of evaluation operationalised by the conferences - the contested boundary between 'engineering' and 'research', in his words. More forcefully, Julia argues that being accepted to top conferences is often more to do with luck than much else - "In the daily life you get really pissed off by this process, and hate it, especially if you get bad reviews. I think you also feel that you are unlucky with the reviewers. and you can also be unlucky. on the other hand you can be lucky and something gets accepted which is actually not good." (Interview 3, May 2019) She is quick, though, to follow this with a somewhat positive appraisal of the overall process: "Of course it is not an ideal option, and their are many disadvantages to the reviewing processes, but I cannot think of something much better." (ibid) Sebastian views these tests in a similar light, pointing to their imperfections but ultimately viewing these as unavoidable:

> "*how to value the degree, how to value a publication and the work someone published, is I guess a very hard challenge* [...] *but there has to be some system and this is the best that is currently out there. peer reviewed conferences with a certain impact factor*." (Interview 6, October 2019)

Though conferences are an imperfect system of valuation, and built on a limited understanding of value, they are generally seen to be a good solution to this most difficult of problems: providing a fair evaluation of a work's worth.

7.3.2.2 Funding

While, then, accounts of conferences generally portray these institutions as both useful and influential, if also imperfect, descriptions of funding processes are almost entirely critical in character. Many of the researchers acknowledged applying for funding as being a central part of their research within SBA. This is an important initial step for all of the researchers - they need to secure funding so that they can proceed with the rest of their research. Simon describes the general requirement:

> *We have some basic funding, but we are also requested to write some applications*

> *ourselves, because we don't have infinite funding, we of course, every PhD student should write an application of fundraising for their own PhD.* (Interview 5, June 2019)

While most of those I spoke to had already received funding for their PhD's,, Laura has recently applied for hers. She describes her current situation:

> *Well we have written a proposal that is under revision. So we are waiting for the reviewers right now, I don't know what happens. Emm but yeah we will see and if it will be accepted then it is good, so we are funded, or otherwise we are going to write another proposal more into the security for engineers direction, lets say.* (Interview 1, May 2019)

Lucas claims that this situation is quite a typical one for researchers in SBA: "At least in our organisation you are a few years in the beginning of your PhD busy with writing proposals because you have to get your own money for doing your PhD. So then maybe after two or three years you are lucky and you have money doing your research." (Interview 4, May 2019) This 'test' then acts as a preliminary determination of the researchers' work's worth, and once passed gives them the financial means to conduct their research, publish work at conferences and finish the PhD.

Overall funding agencies were seen in a negative light by the researchers and they were regularly critiqued throughout the interviews. Lucas, for example, repeatedly complained about the 'nonsense' he was subjected to while applying for funding. Even Julia, who was generally the most positive about the working environment in SBA and academia, agreed that the funding schemes were 'annoying'. Laura arguably makes the strongest critique, saying that if she had to change one thing to improve information provision it would be the funding system for research. *"*If I could change anything, I would like to solve the funding issue [...] in order to be free to make research, actually, and to not have to use your time writing applications.*"* (Interview 1, May 2019)

What accounts for this annoyance? What particular grievances do the interviewees develop? One aspect that Laura in particular highlights is the conflict between the certainty demanded of researchers by funding agencies, and the uncertainty that to her is a fundamental

characteristic of research. In her words:

> *That's actually the biggest problem, that research is not of course something that you can predict. If I would already know what I am doing I would not be doing it. And this is the problem because I have to write an application and I have to pretend that I have a very clear plan although it might very likely change. And a lot of things I might not know yet. I want money for something that is not yet researched, very often, so it is very hard to write an application for that.* (ibid)

Julia sees the problem in quite a similar light saying that "it's not that easy I guess especially because those proposals last for one to six years depending on how huge the projects are and it is kind of hard to predict what the future will bring" (Interview 3, May 2019). Sebastian made a similar argument, with reference to historical fields of study that have now proven valuable for research into blockchain:

> *Works in the area of distributed systems where they had some impossibility results does not hold for certain constructs in the 80s or the 90s, back then it was 'yeah, ok interesting curiosity' and in late 2013 or 14 it received the Dijkstra Prize or so together with another publication. So it is really hard to assess the value of these things* (Interview 6, October 2019)

Lucas, perhaps the most critical of the interviewees of the overall research system, focuses on a different aspect: the need for researchers to "convince the funding body that the funding money is not wasted." (Interview 4, May 2019) He specifically looks at how the need for researchers to continually justify their worth to funding agencies does not diminish throughout a particular career, which he sees as being particularly problematic.

> *But I think if you have a track record* [...] *for example, my supervisor has a PhD and a high number of citations and is very well established in the community and has a track record and has proven that he knows his stuff and does not waste money and so on.* (ibid)

Other critiques focused more on the influence of funding on the type of research carried out in information security, and thus ultimately the type of security that gets practised here. Sebastian is most direct in this regard - focusing on how funding schemes enact an economic valuation of research.

> *you have a funding agency which has to decide whether something is valuable to fund or worth to fund and this does not just depend on the scientific quality on the person that is trying to get the grant or the scientific quality of the grant itself it of course depends on other issues like is it economically valuable to fund this* (Interview 6, October 2019)

This is the most direct insight we get into the particular form of valuation that the test of getting funding enacts - one where the economic worth of a piece of research is dominant, rather than if it "is scientifically very interesting" or the researcher has "a good track record". Furthermore, this economic valuation of work in information security has been a common, if diffuse, thread within the different value practices within the thesis. The critical activity of actors is seen to support particular economic actors, while the worth of a piece of research was also justified according to its contribution to economic growth. An open question, though, regards whether the determination of a source of these practices by one interviewee is sufficient for determining a 'regime of valuation' - an institutionally embedded notion of value that impacts upon an actor's value practices, an issue returned to in the following discussion section.

Markus provides a more general argument in a similar vein, highlighting the focus on 'buzzwords' when writing a grant proposal, as well as how limited these topics are: "Well I think there is much more going on with technology and security then this four or five buzzwords, [...] we are not able to understand all the things completely*"* (Interview 2, May 2019). He argues that funding is offered for proposals that are related to a number of buzzwords, and that this form of valuation overlooks important areas in the development of technology. He did not, though, specify which areas these might be. Simon gives a similar criticism arguing that current funding priorities are inadequate to the difficult tasks that face humanity, though he combines this with a more prescriptive stance, specifically arguing that more funding for social sciences is necessary.

> *I see on a global scale technology progress outperforming human development, so I think we should actually fund more philosophy and psychology areas, so the social sciences, which I think are incredibly important and also incredibly underfunded compared to the technical sciences.* (Interview 5, June 2019)

Again funding mechanisms are critiqued because of their fundamental role in enacting what is valuable research; here it is the valuing of technical sciences that is seen to contribute to some of humanity's deepest issues.

Important to note, though, is that these critiques of funding impacting on the scope of research operate on a very general level, and many of the researchers also downplay the impact of funding bodies on the research that they actually carry out. This is seen again with Simon who refers to this relationship between writing proposals and actual research as one of 'spinning' - where proposals can be written in a way that emphasises one sought after aspect of research, while the researcher themselves are actually more interested in some other part of the work. *"*Although your real main focus is somewhere else, but you just frame it in a way that the funding agency is like - 'ah yeah that's very important research and we like it because blockchain'" (Interview 5, June 2019). Markus gives a similar account of the process: "If you do a proposal with this buzzwords and bring them in the right order and write some nice story about it, then you have a good opportunity that it will be accepted*"* (Interview 2, May 2019). This raises an interesting tension about the different characteristics of various valuation practices and, particularly, justifications, making non-obvious the relationship between these practices and the emergence of research concerns: are some of these justifications 'spin', or do they substantially relate to the process of pursuing worthwhile research?

Comparing the position of conferences and funding raises important issues. Their positions are in many ways the inverse of each other: conferences are in general both the more influential test and are also the less controversial, while funding mechanisms are generally portrayed negatively and the researchers present a number of ways for their influence to be undermined. This finding is not particularly surprising, perhaps, but it is worth thinking through: that more legitimate tests can also be more effective as they are less contested, and their notion of value thus more taken for granted.

Taken together these findings will have hopefully provided a rather detailed account

of the value practices engaged in within SBA Research. Firstly, the research conducted in the centre was conceptualised as a practice of a critique, and, as such a particular enactment of value. Within this, the role of the critiques n enacting their subjects as responsible for security was focused upon. Then, through the notion of justification, the multiple ways that the researchers themselves value their work was outlined, with three registers - a) protecting users b) supporting innovation and c) fulfilling personal demands - outlined. Finally, the institutional environment tht researchers operate within outlined. Here it was found that while SBA Research was perceived to have a relatively heterarchical ordering of value, the value of work remained institutionally determined by being accepted for conferences and getting funding. Altogether this points to the complexity of value practices present within SBA Research, which in a non-linear fashion, amount to specific forms of security being performed in the centre.

8. Discussion

Having presented the central findings of this thesis, this final section will explore their implications and put them in direct conversation with the various literatures outlined in the earlier chapters of the thesis: critical security studies, science and technology studies, valuation studies and the sociology of critique. I will begin by looking at how this thesis contributes to the literature in valuation studies, exploring particularly how the deflated notion of test here is useful in understanding the complex institutional arrangements that perform specific orderings of value, and allow for the reproduction of particular practices of (in)security, while also discussing the difficulties in delineating a coherent regime of valuation. The rest of this section will explore some implications of information security researchers being conceptualised as critical actors: firstly, how this relates to literature in critical security studies and, secondly, to different approaches to the notion of critique. The section, and the thesis as a whole, will end with some thoughts and recommendations on the reflexive tensions this study raises for STS's own critical activities.

8.1 Balancing and ordering value practices

I will first look at the main answer to my research question - the emergence of research focuses within information security research - in the context of literature from valuation studies. I will outline the central finding of simultaneous multiplicity and orderings, discuss how this challenges certain theorizations, while also acknowledging the limits of these findings. These will then be related to my overall research interest - the contemporary provision of information security.

In answering my main research question about the emergence of research focuses in information security research, two value practices emerged in the data as partially explanatory - the multiplicity of personal justifications offered by the researchers through which the perceived value of the piece of work is outlined, and the two institutionalised tests which the work is then subject to. The values enacted through the justifications are quite diverse, while those enacted by the tests were seen to be quite specific in character - an

economic valuation dominated with funding, while 'scientific merit' dominated within conferences. Thus here we have, if we return to David Stark's terminology, simultaneously a heterarchical and hierarchical organizational structure - where a multiplicity of valuation practices are nevertheless constrained by specific institutionally embedded renderings of value. Indeed this is matched in the interviewees' reflections about the conditions of working in the research centre - with a perceived relative heterarchy, while also pointing to the specific determinations of worth by institutional mechanisms.

What this most clearly points out is the limits of any straightforward delineation between heterarchical and hierarchical orderings of value. While I am hesitant to overgeneralize, it seems likely that both heterarchical and hierarchical orderings of value are present in all but the most extreme situations, and that the focus of analysis should be on their complex interactions, rather than some clear cut classification. This case study also, though, points to the limits of a simple normative support for heterarchical forms of organization. While the researchers do share Stark's support for the relatively heterarchical organization found in research, compared with the more hierarchical industry, I would make a contrasting argument: that here we can also see how certain forms of *multiplicity can allow for the uncontested reproduction of valuation practices.* The point is quite simple: with the researchers balancing between personal and institutional valuations, personal commitment to a work is ensured, while the work also continues to operate along institutionally legitimated lines. Furthermore, with a multiplicity of personal justifications deemed legitimate, the orderings of these processes are occluded, and their contestation becomes, to some degree, more difficult.

The question then arises about what specific valuation practices are being institutionally reproduced - what enactments of valuation appear to be those most stable across the researchers accounts, accounts of their institutional environment and potentially also across the discipline of information security research. One useful way of determining this is with reference to Fochler, Felt & Mueller's (2016) notion of 'regimes of valuations' - that is the "discursive, material and institutional background [a] concrete evaluation draws on" (Fochler, Felt & Mueller, 2016, p. 180). With this concept the relationship between the individual and institutional value practices outlined above can be discussed.

While this will be rather circumspect, two such regimes were identified through both their presence in tests and in the researchers own value practices. The first regime identified

was *economic valuation of information security.* This was identified as being a central way that funding schemes determined the value of work – directly identified as such by Sebastian. Throughout the interviews this valuation was also practised continuously by the researchers themselves. Most clearly this can be seen in the justification offered for the researchers work centred around 'engendering trust in digitalisation' - the benefits of which were usually (though not always) constructed in economic terms. The specific form of the critical activities engaged in by the researchers can also be seen as operating within this regime of valuation – with firms as central targets of the researchers' institutionalised critical practices.

The second regime of valuation identified is the *scientific valuation* of information security. Again this was identified as being enacted in a particular test – conferences – with many of the researchers pointing to conferences being focused on 'research' or 'science'. Researchers often drew upon this also when valuing their own research, though often in rather indirect ways. Markus most clearly gave some indication of the specific characteristics of this regime, when explaining why his work was not worthy of a top conference – he said it was more engineering than research, but no specific register of justification can be directly linked with this regime of valuation. This regime can, though, again point to the specificity of the form of critical activity found within information security research – that the subject of critique were often scientific actors responsible for developing digital protocols, systems or technologies, while the different forms that the critiques take – penetration tests as opposed to hacking, emphasis in some domains on mathematical formalism – can also be linked to this regime of scientific worth.

This delineation is of course very brief and superficial. The central aim of this thesis – which was ultimately a rather exploratory step into quite a foreign and understudied field – was the identification of more concrete value practices: critiques, justifications and tests. These regimes of valuation point to broad coherences in the field, which would be a useful starting off point for further research, that could explore in far more detail the material, discursive and institutional background that the researchers operate within. Nevertheless, certain broad regimes of valuation and coherent practices of value have been identified as operating within this specific site within the broader field of information security. These regimes of valuation also, ultimately, point in important ways to how (in)security is performed within this site - how issues become prioritized in the discipline, how certain methods are deemed appropriate, and how different groups are enacted as responsible for

providing security within various (digital) domains.

8.2 (In)Security as a (Multiple) Critique

This section will move on to explore the implications of this thesis and its findings for critical security studies (CSS). It will first look at the application of a theoretical framework derived from Luc Boltanski and valuation studies within a literature where Bourdieu is a more common reference point. Secondly, the conceptualisation of these security actors as critical will be related to literature within different strands of CSS.

8.2.1 Multiplicity and CSS

This thesis was situated within literature from the Parisian school of critical security studies. A central project within this has been the empirical study of different worlds of security practices - various sites within more or less traditional security institutions (security agencies, police, military) were empirically investigated (McCluskey, 2017). One of the main contributions that this thesis makes to this literature is highlighting the *multiplicity of practices that operate within a particular security world*. Restating a central argument from the literature review, this Parisian critical security studies literature is often informed by a Bourdieusian theoretical framework (Bigo, 2011) and, as such, the social worlds that are explored in these studies are often rendered internally homogeneous. One contribution of this thesis and its findings is to complexify this picture by pointing to the multiplicity of valuation practices within this particular world of security. It has been shown have how the valuation practices - and the attendant constructions of (in)security, referent objects, responsible actors - are thoroughly complex and messy: the actors' valuation practices are not determined by their position within a field of security - rather they are active and reflective and have numerous practices of valuation though which they can enact the worth of their research. Further, no one referent object remains in place for the actors, at different times technologies, users, companies or innovation itself takes this place. Ultimately the notion of security and (in)security itself has multiple meanings within this one social space - from physical harm, to centralization, to a (dys)functional economy.

An important stress in this thesis has also, though, been that the multiplicity here is a highly specific phenomenon. On one level this refers to the generalizability of this finding - it should be noted that the case explored here is rather idiosyncratic one compared with other

studies conducted within critical security studies. Returning to a quote from Emma McLuskey: "ethnographic CSS [...] has, though enlarging the meaning of 'security', nonetheless tended to operate within a predefined space and a somewhat preconceived notion of what a 'security' site of research should look like." (2017, p. 3) Furthermore the research into the relationship between security and technology has often focused on the use of technologies by more-or-less traditional security institutions, concerned with policing, border control, exploring how the use of big data and algorithms changes these practices. Information security research is not a traditional space of security. This research centre is not part of any state security apparatus, the links between it and the military, police etc. are rather indirect, the concerns here are not immediately about deviance or control. The security actors in this case mostly approach technology from a different perspective - how do we make the technologies themselves secure, rather than how these technologies can be used in a secure fashion. What this should underline is that the finding of multiplicity and heterarchy within this specific site is not necessarily one that can be generalized across the whole spectrum of security provision. Indeed this was stressed by the researchers themselves, who argued that scientific research in general and particularly at this centre, was characterised specifically by an openness to different forms of valuation and a freedom in their research practices. The extent and form of multiplicity found in other sites of security remains an open question.

8.2.2 Critique and CSS

Another finding important to relate to the critical security studies literature is that the primary practice of (in)security found in the research centre is one of critique. This highlights the specificity of previous conceptualisations of security practices - particularly securitization theory - and points also to important reflexive tensions for the critical study of security.

The finding that the central security practise engaged in by the researchers is one critique, relates to the prominence given to processes of threat construction within securitization theory and critical security studies more generally. For the Copenhagen School authors, security was fundamentally about constructing a threat - which was in some sense external to the audience to the pronouncement was directed towards. This is seen in this standard definition of securitization: "when a securitizing actor uses a rhetoric of existential threat and thereby takes an issue out of what under those conditions is "normal politics," we have a case of securitization" (Buzan et al., 1998, p. 24-25). This thesis can be seen to be a

further contribution to the broad empirical project that has tried to challenge some of these assumptions within the original securitization theory framework. With the particular form of critical (in)security practiced within the research centre, the focus is less on external threats, and moreso on internal failings and vulnerabilities. The researchers generally focus on particular devices, software, protocols or business practices, and highlight the problematic security implications that emerge with these. That is not to say that information security research is entirely exempt from processes of threat construction, and indeed, one example of this practice within the research centre was presented: Markus creating honeypots to attract and analyze the behaviour of attackers. This exception, though, proves the general rule - that the researchers here were more focused on identifying internal insecurities and vulnerabilities, than with focusing on external threats. With this case the boundary between analyses focusing on risk and those focusing on (in)security becomes increasingly blurry.

In line with this the researchers' critiques largely focused on actors who they could engage with, and whose practices they wanted to improve, rather than being focused on attackers, for instance. On some level this says something about critical activity itself - that as a negative evaluation of a certain actor's behaviour, it often acts as to encourage this actor to improve their behaviour in some way: it would on some level not make semantic sense if the researchers would critique the attackers. So while critique may indeed necessitate some external vantage point, as Boltanski argues, so too is it usually in some sense internal - which separates it from security as theorized by the Copenhagen school. Following this, the implied solutions to these problems thus also switches. Rather than needing the issue to be moved out of normal politics into a nondemocratic space, the solution to these vulnerabilities simply comes with improved practices by the groups critiqued. This extends Balzacq, Léonard and Ruzicka's (2016) argument about the often unexceptional nature of certain security practices and the overlaps between studies of risk and those of security.

Understanding these security actors as critical also upsets certain assumptions within Parisian Security Studies. Centrally, the actors were found to be more reflexive than these studies accounted for - multiple registers, yes, but also their own situation critiqued and contested from the inside (to some degree). Important here is the inclusion of the critical activities engaged in from outside of their research - where the boundaries and political implications of the researchers work was questioned by some of the interviewees – and also the researchers own critiques of the tests that evaluate their work. Garfinkle's (1967) 'cultural

dope' is partially replaced by the 'cultural critic', who is reflexive and challenges their own situation. A further implication of this is to question the boundary constructed between critical security studies and other, presumably non-critical, security students and actors. Following the previous point, if these actors can also engage in critiques of the security environment, how does this change the critical role of analysts? And, more problematically, what happens when it is discovered that critique plays a constructive role within the institutions being critiqued and that it is even actively cultivated by these institutions? How can these critical activities be differentiated? These reflexive issues raise fundamental questions about researchers' critical engagements with both security and research institutions, and the final section of the thesis will be dedicated to them.

8.3 Critique as (In)Security

If the last section explored the implications of security actors being critical for the (critical) study of security, this section will look at the implications of this finding for the study of critique. We will look at how the different pragmatic theories of critique are able to cope with this empirical case, and dwell on how these critical activities challenge both STS's - and my own - critical repertoire.

This thesis is situated within two related, but ultimately divergent, understandings of critique: Boltanski's sociology of critique, and Latour's polemics against the contemporary critical scene. Restating from the theoretical section: both of these are grounded in concerns about Bourdiean critical sociology being overly deterministic and the subsequent epistemic privileges that are granted to sociologists. As such, they both argue for a deflated role for these sociologists; focusing on local empirical work they should emphasise the agency of those being researched and develop a 'pragmatic' sociology. They diverge, though, in their evaluation of the critical activities carried out by non-academic actors, and the implications of these for academic work. Boltanski is broadly positive about the role of critique in society - seeing it as, amongst other things, an important catalyst for progressive social change. He moreover worries that a purely pragmatic sociology might hinder the critical capacities of vulnerable actors in society. Latour is more negative. He cites the growth of conspiratorial thinkers, sceptical of science and, taking his example, climate change, as a concerning employment of critical strategies. He is particularly concerned about a strong form of critique used by these actors, where certain people's beliefs are unmasked as fetishes produced by

particular social forces - a move he refers to as 'barbaric'.

One task of this thesis was to contribute to these discussions with an agnostic empirical investigation into a rather idiosyncratic group of critical actors - information security researchers. Having presented the findings, what can now be said about these different understandings? Who presents the more tenable position? In a word: neither (or, indeed, both). The undifferentiated support given by Boltanski appears problematic given, to take just one issue, the contradictory nature of the critiques formulated by the researchers. To take the clearest example of this, it was in general found that the research-critiques were formulated to benefit the process of technological innovation, particularly digitalisation, allowing this to securely develop. Yet other non-institutional critiques questioned this process of innovation, highlighting the negative effects this has on different social groups, for instance. Given Boltanski's toolkit these critiques should both be supported, which appears untenable. Furthermore, the symbiotic relationship between the critical research activity and particular forms of digital capitalism, seem at odds with the sociologist's commitment to 'political emancipation'.

Latour's position, though, also faces difficulties. Some of the critiques formulated by the researchers seemed to positively resonate with Latour's favoured critical activity. As Guggenheim phrases it "Thus, the descriptions of Marxists and economists, of philosophers of science and Marxist critics of science, etc., are equally wrong, because they do not match the empirical complexity of the world." (2019, p. 70) Compare this with the numerous critiques given by the theorists that argued that their empirically complex studies undermined the overly theoretical work of the designers of technologies. Moreover, the positive relationship between the researchers' critiques and their targets accords with Latour's appeal for a more constructive criticism: "The critic is not the one who debunks, but the one who assembles [...] the one for whom, if something is constructed, then it means it is fragile and thus in great need of care and caution." (p.246). As critics who note the fragility of various devices, thus contributing to their further assemblage, information security researchers could be a model for the critical activity Latour envisages. Other critiques that they offer, though, seem closer to the 'barbaric' unmasking forms of critique. He denounces, for instance, "the addition of something more human that the inhumane matters of fact would have missed" by critical actors (2004, p. 246). What then to make of Simon's view that more humanity within technological sciences is exactly what is needed? Should we unmask this position as a fetish,

or simply ignore it? Or what about Markus's preference for a strong critical activity to come from the social sciences – one that unmasks and denounces current technological development? What should we do when the subjects we are studying contradict our own apparently democratic critical activities? Latour's position seems problematic, on the one hand, as it arbitrarily empties the actors of a large portion of their critical repertoires. Moreover it is these stronger critiques that challenge the direction and functioning of information security research, and his decision to exclude them has, in this situation at least, decidedly conservative implications.

So we are at something of an impasse. Helpful at this point is perhaps to make explicit my own critique of information security research that I have up to this point been somehwat implicitly been formulating. This is, put simply, 'it could be otherwise". This short phrase, according to Woolgar & Lezaun (2013), has been a guiding normative slogan for much STS work, helping to organise the political logic performed in this work. That is, showing the historical contingency of a particular set of practices undermines the perceived naturalness of a given phenomena and argues that these practices can also be transformed. Unsurprisingly, then the same also applies to information security research. The work that arises here is specific in nature - as seen with the distinct critical activities conducted within the research centre as compared to those outside. This specificity also has a particular historical, institutional origin: seen as emergent from various valuation practices. The critical import of all of this is that it could be otherwise. That the critical activities engaged in by the researchers could be changed somehow to bring about more desirable research, realities, worlds.

Once again, though, the next steps do not appear particularly easy or obvious. On one level - how can these worlds be brought into being? How can this critical work gain traction? And, more fundamentally - what worlds do we ultimately want to bring into existence? Which critiques do we want to lend our support to? And, as always, on what basis can we decide? While this thesis is not the place for such intractable problems to be solved I do think that, in the case of information security research at least, recent arguments to experimentalise STS's methodologies appear a promising avenue of further work. Michael Guggenheim outlines the rationale behind these contributions as:

this empirical outlook is not guided towards a critique of theories, but towards an

> *experimental modification of practices with the help of various devices. Unlike in critical social science, speculative practitioners do not denounce practices, nor do they try to change practices according to a given theoretical standard. Rather, inventive or speculative methods are employed to change the world in unforeseen directions. They begin with the insight that in moments of controversy, the social world is performatively opened up.* (Guggenheim, 2019, p. 70)

In the context of information security this would mean enacting a controversy within information security, encouraging the researchers here to present their moral activities, to try and engage with and challenge the limitations of their own discipline, and to come up with novel ways that these can be changed. Concretely, this could involve a somewhat reconfigured focus group where the answers to the above questions would be collaboratively sought - what kind of security should information security researchers practise, what type of critical activity should be engaged in, who should be protected and empowered through research - while also pursuing ways for these to be materialised – particularly surrounding the questions of how information security research is governed and evaluated. Ultimately this would be an exercise in 'critical companionship' (Austin, Bellanova, & Kaufmann 2019) – making explicit the always collective process of critique. Thus, underlying this proposal is a fundamental, if difficult to justify, finding from this thesis: that information security researchers (at least those I spoke with) would make worthy companions in critique, and, following a central finding from this thesis, that the responsibility and agency given to them through such a critical practise would be well merited.

While this is, in essence, a proposal for future research, I also hope that this thesis can in itself be a small contribution to such a development of critical activities. By providing a detailed account of the critical research carried out by a group of (in)security actors who are not usually understood in these terms, I hope to have encouraged some further reflection on how this term is used both in the technical and social sciences, how we understand the specificity of our own critical activities and, ultimately, how these might in future be consciously cultivated.

Bibliography

Aradau, C., & Huysmans, J. (2019). Assembling credibility: Knowledge, method and critique in times of 'post-truth'. *Security Dialogue*, *50*(1), 40-58.

Austin, J. L., Bellanova, R., & Kaufmann, M. (2019). Doing and mediating critique: An invitation to practice companionship. *Security Dialogue, 50*(1), 3-19

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: Theory and cases. *International Relations*, *30*(4), 494-531.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), 147-164.

Bigo, D. (2008) Globalized (in)security: The field and the ban-opticon. In: D. Bigo & A. Tsoukala (Eds.), *Terror, insecurity and liberty: Illiberal practices of liberal regimes*. (pp. 10-42). Routledge

Bigo, D. (2011). Pierre Bourdieu and International Relations: Power of practices, practices of power. *International Political Sociology, 5*(3): 225-258.

Bigo, D. (2014). The (in) securitization practices of the three universes of EU border control: Military/Navy–border guards/police–database analysts. *Security Dialogue, 45*(3), 209-225.

Bigo, D., & McCluskey, E. (2018). What Is a PARIS Approach to (In) securitization? Political Anthropological Research for International Sociology. In: A. Gheciu & W. C. Wohlforth (eds.) *The Oxford handbook of international security* (pp. 116-132) Oxford University Press.

Boulding, E. (1981). Perspectives of women researchers on disarmament, national security, and world order. *Women's Studies International Quarterly*, *4*(1), 27-40.

Boltanski, L., (1987 [1982]). *The making of a class: Cadres in french society*. Cambridge University Press.

Boltanski, L., Chiapello È. (2005 [1999]). *The new spirit of capitalism*. Verso.

Boltanski, L., Thévenot, L., (2006 [1991]), *On justification: The economies of worth*. Princeton University Press.

Boltanski, L. (2011 [2009]), *On critique: A sociology of emancipation.* Polity Press.

Bueger, C., & Gadinger, F. (2015). The play of international practice. *International Studies Quarterly, 59*(3), 449-460.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Byrne, B. (2004). Qualitative interviewing. *Researching Society and Culture, 2,* 179-192.

C. A. S. E. Collective (2006). Critical approaches to security in Europe: A networked manifesto. *Security Dialogue, 37*(4), 443-487.

Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, *6*(2), 22-30.

Cavelty, M. D., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review, 15*(1), 37-57.

CBS News (2017) *Global cyberattack strikes dozens of countries, cripples U.K. hospitals.* https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). Sage.

Cooke, J. (1992). Formal Methods–Mathematics, Theory, Recipes or what?. *The Computer Journal*, *35*(5), 419-423.

Davidshofer, S., Jeandesboz, J., & Ragazzi, F. (2016). Technology and security practices. *International Political Sociology: Transversal Lines*, 135.

De Goede, M. (2018). The chain of security. *Review of International Studies*, *44*(1), 24-42.

de Leeuw, K. M. M., & Bergstra, J. (Eds.). (2007). *The history of information security: a comprehensive handbook*. Elsevier.

Decentralized Systems Group (n.d.) *About*. https://blockchain.sba-research.org/#about

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3-4), 189-198.

Dussauge, I., Helgesson, C. F., & Lee, F. (Eds.). (2015). *Value practices in the life sciences and medicine.* Oxford University Press,

Eilam, E. (2005). *Reversing: secrets of reverse engineering*. John Wiley & Sons.

European Commission (2019) *Building strong cybersecurity in the European Union: resilience, deterence, defence.* https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence

European Defence Agency (2017) *Cyber Defence*. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

Evans, S. W., & Frow, E. K. (2015). Taking care in synthetic biology. In B. Rappert & B. Balmer *Absence in science, security and policy* (pp. 132-153). Palgrave Macmillan.

FeatureCloud (n.d.) *Our Vision*. https://featurecloud.eu/about/our-vision/

Fochler, M., Felt, U., & Müller, R. (2016). Unsustainable growth, hyper-competition, and worth in life science research: Narrowing evaluative repertoires in doctoral and postdoctoral scientists' work and lives. *Minerva, 54*(2), 175-200.

Foucault (1984) What is Enlightenment? In P. Rabinow (Ed.), *The Foucault Reader* (pp. 32-50). Pantheon Books.

Fowler, B. (2014) Figures of Descent from Classical Sociology: Luc Boltanski. In: Susen, S., & Turner, B. S. (Eds.). *The spirit of Luc Boltanski: Essays on the 'pragmatic sociology of critique'*. Anthem Press.

Fuller, S. (2018). What can philosophy teach us about the post-truth condition? In: M, A. Peters, S Rider, M. Hyvönen & T. Besley (Eds.), *Post-truth, fake news* (pp. 13-26). Springer.

Geertz, C. (1973). Thick description: Toward an interpretive theory of culture. In: Y. S. Lincoln, N. K. Denzin (Eds.), *Turning points in qualitative research: Tying knots in a handkerchief* (pp. 143-168). Altamira Press.

Galtung, J. (1969). Violence, peace, and peace research. *Journal of peace research*, *6*(3), 167-191.

Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41-73.

Guggenheim, M. (2019). How to use ANT in inventive ways so that its critique will not run out of steam?. In A. Blok, I. Farias & C. Roberts (Eds.) *The Routledge Companion to Actor-Network Theory* (pp. 64-72). Routledge.

Guggenheim, M., & Potthast, J. (2012). Symmetrical twins: On the relationship between Actor-Network theory and the sociology of critical capacities. *European Journal of Social Theory, 15*(2), 157-178.

Grint, K., & Woolgar, S. (1992). Computers, guns, and roses: what's social about being shot?. *Science, Technology, & Human Values*, *17*(3), 366-380.

Hansen, L. (2000). The Little Mermaid's silent security dilemma and the absence of gender in the Copenhagen School. *Millennium*, *29*(2), 285-306.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly, 53*(4), 1155-1175.

Heuts, F., & Mol, A. (2013). What is a good tomato? A case of valuing in practice. *Valuation Studies, 1*(2), 125-146.

Huysmans, J. (2011). What's in an act? On security speech acts and little security nothings. *Security dialogue*, *42*(4-5), 371-383.

IEEE Symposium for Security and Privacy (2019b, June 3) *IEEE S&P 2019—40th Celebration Plenary Session: Panel: Reflections on four decades of the symposium* [Video]. Youtube. https://www.youtube.com/watch?v=O8FTDljb_jM

IEEE Symposium for Security and Privacy (2019a, June 3) *IEEE S&P 2019—40th Celebration Plenary Session: A Wild Ride Through Time* [Video]. Youtube. https://www.youtube.com/watch?v=PgLXbu5VmIU

Jagd, S. (2011). Pragmatic sociology and competing orders of worth in organizations. *European Journal of Social Theory, 14*(3), 343-359.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kerr, P. (2003). *The evolving dialectic between state-centric and human-centric security*. https://openresearch-repository.anu.edu.au/bitstream/1885/42112/2/03-2.pdf

Krause, K., & Williams, M. C. (1996). Broadening the agenda of security studies: Politics and methods. *Mershon international studies review*, *40*(2), 229-254.

Latour, B. (2004). Why has critique run out of steam? From matters of fact to matters of concern. *Critical inquiry, 30*(2), 225-248.

Leese, M., Lidén, K., & Nikolova, B. (2019). Putting critique to work: Ethics in EU security research. *Security Dialogue, 50*(1), 59-76.

Lisle, D. (2014) Energizing the International. In: Acuto, M., & Curtis, S. (eds,). *Reassembling International Theory: Assemblage Thinking and International Relations*. (pp. 67-74). Palgrave MacMillan

Lunning, S. (2013) *Anthropologists in the company of gatekeepers.* Leiden Anthropology. https://www.leidenanthropologyblog.nl/articles/anthropologists-in-the-company-of-gatekeepers

MacMillam, M. (2011) *A Short History of Secrecy*. Foreign Policy. https://foreignpolicy.com/2011/02/21/a-short-history-of-secrecy/

Mathematics for Testing, Reliability and Information Security (n.d.) *MaTRIS.* https://matris.sba-research.org/

McCluskey, E. (2017). Everyday (in) security: A bibliography. *Working Papers in Urban Language & Literacies*, *214*.

McDonald, M. (2008). Securitization and the Construction of Security. *European journal of international relations, 14*(4), 563-587.

McDonald, N. (n.d.) *Past Present and Future Methods of Cryptography and Data Encryption*. The University of Utah. https://my.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf

Miller, C. A. (2015) Globalizing Security: Science and the Transformation of Contemporary Political Imagination. In: S. Jasanoff, S. Kim (Eds.) *Dreamscapes of Modernity: Sociotechnical imaginaries and the fabrication of power.* (Pp 277-299). University of Chicago Press.

Mol, A., & Law, J. (1994). Regions, networks and fluids: anaemia and social topology. *Social studies of science*, *24*(4), 641-671.

Murphey, D. (2019) *A history of information security*. IFSEC Global. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Möllers, N. (2017). The Mundane Politics of 'Security Research'. *Science & Technology Studies*, 14-33.

Odlyzko, A. (2003). Economics, psychology, and sociology of security. In *International Conference on Financial Cryptography* (pp. 182-189). Springer.

O'Neill, B. (1994). Game theory models of peace and war. *Handbook of game theory with economic applications*, *2*, 995-1053.

Online Trust Alliance (2019) 2018 *Cyber Incident and Breach Trends Report*. Internet Society https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf

Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies, 35*(1), 5-32.

Rid, T. (2016) *How Russia Pulled Off the Biggest Election Hack in U.S. History*. Esquire. https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/

Rishi, R., Saluja, R. (2019) *Future of IoT.*: EY. https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/$FILE/EY-future-of-lot.pdf

Salter, M. B. (Ed.). (2015). *Making things international 1: Circuits and motion*. University of Minnesota Press.

SBA Research (n.d.a) *About.* Retrieved from: https://www.sba-research.org/about/

SBA Research (n.d.b) *Image Folder.* https://www.sba-research.org/wp-content/uploads/2016/10/SBA-Research_Imagebroschüre_2016_ONLINE.pd

Schneier, B. (2016) Integrity and Availability Threats. https://www.schneier.com/blog/archives/2016/01/integrity_and_a.html

Schneier, B. (2017) Security and the Internet of Things. https://www.schneier.com/blog/archives/2017/02/security_and_th.html

Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*, *6*(2), 31-40.

Simon, S., & de Goede, M. (2015). Cybersecurity, bureaucratic vitalism and European emergency. *Theory, Culture & Society, 32*(2), 79-106.

Stark, D. (2000). Ambiguous assets for uncertain environments: Heterarchy in postsocialist firms. *Экономическая социология, 1*(2).

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy*, *33*(1), 148-170.

Stone, J. (2013). Cyber war will take place!. *Journal of Strategic Studies, 36*(1), 101-108.

Suchman, L., & Weber, J. (2016). Human-machine autonomies. In: N. Bhuta, Beck, R. Geiβ, H. Liu, C. Kreβ (Eds.) *Autonomous weapons systems: law, ethics, policy.* (pp. 75-102.) Cambridge University Press,

Swartz, D. (1997). *Culture and power: The sociology of Pierre Bourdieu*. University of Chicago Press.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

Wæver, O. (1993). Securitization and desecuritization In: Lipschutz, R. D. (Ed.). *On security*. (pp. 48-81). Columbia University Press.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security.* Cengage Learning.

Witjes, N., & Olbrich, P. (2017) A fragile transparency: satellite imagery analysis, non-state actors, and visual representations of security. *Science and Public Policy 44*(4), 524-534.

Wohlforth, W. C. (2009). Realism and security studies. In: T. Balzacq, M. D. Cavelty (eds.) *The Routledge Handbook of Security Studies* (pp. 25-36). Routledge.

Woolgar, S., & Lezaun, J. (2013). The wrong bin bag: A turn to ontology in science and technology studies?. *Social studies of science, 43*(3), 321-340.

Appendix A - English Abstract

This thesis is an exploration of the valuation practices present within an information security research centre in Austria. This site offers itself as a case for two overlapping research agendas: the empirical study of knowledge cultures, undertaken by scholars from science and technology studies (STS), and the study of sites of security practise, a focus of critical security studies (CSS). Using a theoretical framework derived from Luc Boltanski and valuation studies, this thesis conceptualises the work of the information security researchers as a specific *critical practice* – one that enacts as responsible for security the actors that the critique is directed towards. The specificity of these critiques is outlined by contrasting them with critical activities engaged in by the researchers outside of academia. The rest of the findings will point to certain valuation practices related to the emergence of this specific form of critique: the justifications that the researchers themselves offer for their work and the tests that enact its institutional value. The thesis will finish on some thoughts regarding the implication of these findings for the (critical) work carried out by scholars from STS, CSS and information security research - pointing particularly to ways that these might be collaboratively extended.

Appendix B - German Abstract

Diese Arbeit befasst sich mit Bewertungspraxen eines Forschungszentrums für Informationssicherheit in Österreich. Diese Fallstudie bietet sich als interessantes Beispiel für zwei sich überlappende Forschungsagenden an: einerseits für die empirische Untersuchung von Kulturen der Wissensproduktion aus Sicht der Wissenschafts- und Technikforschung (STS),, und andererseits zur Erforschung von Sicherheitspraxen, ein Schwerpunkt der Critical Security Studies (CSS). Unter Verwendung eines theoretischen Rahmens, der auf der Arbeit von Luc Boltanski sowie Konzepten aus dem Bereich der Valuation Studies basiert,, wird die Arbeit der Informationssicherheitsforscher*innen als eine spezifische kritische Praxis konzeptualisiert, die die Akteure, auf die sich die Kritik richtet, als für Sicherheit verantwortlich darstellt. Dies steht im Gegensatz zu kritischen Praxen der Forscher*innen außerhalb der Wissenschaft. Die weiteren Ergebnisse weisen auf bestimmte Bewertungspraxen hin, die mit der Entstehung dieser spezifischen Form der Kritik zusammenhängen: die Rechtfertigungen, die die Forscher*innen selbst für ihre Arbeit vorbringen, und die Tests, die den Wert der Arbeit institutionell bestimmen. Die Arbeit schließt ab mit einigen Gedanken zu den Implikationen dieser Ergebnisse für die (kritische) Arbeit von Wissenschaftler*innen aus den STS-, CSS- und aus der Informationssicherheitsforschung und weist insbesondere auf Möglichkeiten hin, wie diese kollaborativ erweitert werden könnten.

Appendix C - Example Interview Guide

Can you tell me a bit about yourself?
- What is your educational background?
- Why did you choose to study this?

How did you become interested in computer science?

How did you become interested in information security?

You are interested in Blockchain
- Could you try to explain what exactly usability is?
- How did you become focused on this topic?
- Do you think this is an important topic to focus on? Why?
- Do you think your work can benefit society? In what ways?

How has your focus changed during your time in information security? What led to these changes?

What are you focusing on for your dissertation?
- Why are you focusing on this?

How did you begin to work for SBA?
- How is it different to other places that you have worked in?
- How do SBA coordinate the different projects that happen here?
  - In what ways does this influence the work that you do? Can you give me an example?

Are you working on many projects at the moment?

Have you got funding for your PhD yet? Can you walk me through the funding process
- Why do you think the funders are interested in your project?
- Did the focus of this project change in the process of getting funding for it? In what way?
- What groups normally fund the work that you do? Do these different funders have different expectations for your project? In what way?
- How do you anticipate what projects might get funding?

How important is publishing at conferences for you?

How do the priorities of the conferences change your work?
Do you think the conference system is a good one? Why?

What other areas in infosec do you think it would be important to study?
Why these areas?
Do you think about changing your focus to one of these areas? How would you go about doing this?

I have read a book by Bruce Schneier, and it was really a mix between a technical diagnosis of information insecurity and policy advice.
What do you think of this type of approach? Is it important?
Do you think it is important to engage with politics and society like he does? Why (not)?

On the homepage of SBA it says that the centre is focused on strengthening Europe's cybersecurity capabilities, how do statements like this relate to your work?
How are the priorities of people working in SBA different from those working for the European Union - in ENISA, for example?

The public imagination of information security I guess is heavily connected with the hacking community.
Does this connection make sense to you?
In what ways are the two communities similar or different?
How do their priorities differ?

Schneier talks about security being an arms race...
How are we doing in this race at the moment?
How is your research helping in this?

What are some general changes would you suggest to improve information security?