Turun yliopisto
University of Turku

PARASITIC ORDER MACHINE

A Sociology and Ontology of Information Securing

Jukka Vuorinen

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
Sarja - ser. B osa - tom. 392 | Humaniora | Turku 2014

University of Turku

Faculty of Social Sciences
Department of Social Research
Sociology
The Doctoral Programme of Social and Behavioural Sciences

Supervised by

Hannu Ruonavaara
Professor of Sociology
Department of Social Research
University of Turku

Seppo Pöntinen
Emeritus Professor of Sociology
Department of Social Research
University of Turku

Olli Pyyhtinen
Professor of Sociology
School of Social Sciences and Humanities
University of Tampere

Reviewed by

Lucas Introna
Professor of Organisation, Technology and Ethics
Department of Organisation, Work & Technology
Lancaster University Management School

Wolter Pieters
Assistant Professor
Section ICT
Faculty of Technology, Policy and Management
Delft University of Technology

Opponent

Lucas Introna
Professor of Organisation, Technology and Ethics
Department of Organisation, Work & Technology
Lancaster University Management School

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

ISBN 978-951-29-5867-2 (PRINT)
ISBN 978-951-29-5868-9 (PDF)
ISSN 0082-6987
Painosalama Oy - Turku, Finland 2014

ABSTRACT

Vuorinen, Jukka
Parasitic Order Machine: A Sociology and Ontology of Information Securing
Turku, Finland: University of Turku 2014

This study examines information security as a process (information securing) in terms of what it does, especially beyond its obvious role of protector. It investigates concepts related to 'ontology of becoming', and examines what it is that information securing produces. The research is theory driven and draws upon three fields: sociology (especially actor-network theory), philosophy (especially Gilles Deleuze and Félix Guattari's concept of 'machine', 'territory' and 'becoming', and Michel Serres's concept of 'parasite'), and information systems science (the subject of information security). Social engineering (used here in the sense of breaking into systems through non-technical means) and software cracker groups (groups which remove copy protection systems from software) are analysed as examples of breaches of information security. Firstly, the study finds that information securing is always interruptive: every entity (regardless of whether or not it is malicious) that becomes connected to information security is interrupted. Furthermore, every entity changes, becomes different, as it makes a connection with information security (ontology of becoming). Moreover, information security organises entities into different territories. However, the territories – the insides and outsides of information systems – are ontologically similar; the only difference is in the order of the territories, not in the ontological status of entities that inhabit the territories. In other words, malicious software is ontologically similar to benign software; they both are users in terms of a system. The difference is based on the order of the system and users: who uses the system and what the system is used for. Secondly, the research shows that information security is always external (in the terms of this study it is a 'parasite') to the information system that it protects. Information securing creates and maintains order while simultaneously disrupting the existing order of the system that it protects. For example, in terms of software itself, the implementation of a copy protection system is an entirely external addition. In fact, this parasitic addition makes software different. Thus, information security disrupts that which it is supposed to defend from disruption. Finally, it is asserted that, in its interruption, information security is a connector that creates passages; it connects users to systems while also creating its own threats. For example, copy protection systems invite crackers and information security policies entice social engineers to use and exploit information security techniques in a novel manner.

Keywords: Information security, Information security threat, Territoriality, Becoming, Social engineering

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Vuorinen, Jukka
Parasiittinen järjestyskone – tietoturvaamisen sosiologia ja ontologia
Turku: Turun yliopisto, 2014

Tämä tutkimus tarkastelee tietoturvaa prosessina eli tietoturvaamisena. Se keskittyy erityisesti kysymykseen siitä, mitä muuta tietoturva tekee kuin suojaa. Tutkimus ponnistaa ”tulemisen ontologiasta” ja sen käsitteistä ja ruotii, mitä tietoturva toimiessaan tuottaa. Tutkimus ammentaa kolmesta eri tieteen haarasta: sosiologiasta (erityisesti toimijaverkostoteoriasta), filosofiasta (erityisesti Gilles Deleuzen ja Félix Guattarin koneen, territorion ja tulemisen käsitteistä sekä Michel Serresin parasiitin käsitteestä) ja tietojärjestelmätieteestä, josta väitöstutkimuksen kohde juontaa juurensa. Sosiaalista hakkerointia ja ohjelmistomurtajia – kräkkereitä – analysoidaan tietoturvan murtumisen esimerkkeinä. Yhtenä olennaisimmista tutkimustuloksista on, että tietoturva on itsessään aina keskeyttävää ja häiritsevää: tietoturva analysoi ja näin keskeyttää jokaisen sen kanssa kosketuksiin tulevan entiteetin siitä huolimatta, oli kyseinen entiteetti sitten haitallinen tai ei. Tämän väliintulon seurauksena entiteetistä tulee aina erilainen (tulemisen ontologia). Tietoturvaaminen pyrkii järjestämään suojeltavat ja suojelevat entiteetit erilaisiksi hallittaviksi alueiksi, territorioiksi. Tietojärjestelmien alueet (esimerkiksi järjestelmän järjestetty sisäpuoli ja järjestämätön ulkopuoli) ovat kuitenkin ontologisesti samantasoisia. Ainoa ero territorioiden välille syntyy siitä, miten ne ovat järjestettyjä. Toisin sanoen haittaohjelmat ovat samanlaisia kuin hyötyohjelmatkin – molemmat käyttävät järjestelmää. Ainoa ero muodostuu niiden suhteesta järjestykseen. Kyse on siis siitä, kuka käyttää järjestelmää ja mihin tarkoitukseen. Toiseksi tutkimus osoittaa, että tietoturva on aina ulkopuolinen lisä suhteessa suojattavaan järjestelmään (näin tietoturvaa voidaan serresläisittäin kutsua parasiitiksi). Kun tietoturvaaminen luo suojaa järjestämisen kautta ja kun se yrittää ylläpitää järjestystä, se tulee luoneeksi suojeltavalle järjestelmälle uuden järjestyksen, joka rikkoo aiemmin olemassa olleen järjestyksen. Esimerkiksi kopiosuojaus on suojattavalle ohjelmistolle täysin ulkoinen tekijä. Kun kopiosuojaus lisätään järjestelmään, siitä tulee erilainen. Näin tietoturva, jonka pitäisi olla häiriöiden poistaja, häiritseekin itse suojattiaan. Tutkimus väittää, että tiedon turvaaminen keskeyttämisineenkin luo yhteyksiä. Esimerkiksi tietoturva yhdistää käyttäjät järjestelmiinsä, mutta se luo samoin myös omat uhkansa. Esimerkiksi kopiosuojaus kutsuu luoksensa kräkkereitä ja tietoturvapolitiikat houkuttelevat sosiaalisia hakkereita. Molemmat, kräkkerit ja hakkerit, keksivät tietoturvalle uuden käyttötavan.

Asiasanat: tietoturva, tietoturvauhka, territoriaalisuus, sosiaalinen hakkerointi, ohjelmistomurtajat

CONTENTS

ACKNOWLEDGEMENTS

This dissertation deals with parasites and machines. I feel as if I've been a parasite myself, because in the course of writing this dissertation I have had a great number of supporting people around me. As a parasite, I have drained thoughts and support. This dissertation itself has been a parasite. It has provided me with moments of delight and anxiety. Although the noisy dissertation parasite has awakened me many times just before dawn, the parasite has also brought me together with wonderful people, provided me with joy, and given me the possibility of expressing myself through it.

First I want to thank my supervisors. Thank you Professor Hannu Ruonavaara. Our thoughts on sociology differ very much. Yet, you have always supported me, read and commented on my papers, lent me your books, and employed me. Thank you. Professor Olli Pyyhtinen, thank you for your support. Countless times I have interrupted your work just to hear and drain your thoughts, just as a real parasite does. Thank you for being so generous in your comments and thanks for being a friend. If someone is going to tackle the unthought it is you, Olli. Emeritus Professor Seppo Pöntinen's support was crucial in the early stages of this project, thank you.

The reviewers of this dissertation gave me a great number of insightful comments. Thank you Professor Lucas Introna for helping me discover what my work is all about: ontology of becoming. I am also thankful that you have agreed to be my opponent. I am truly honoured. Assistant Professor Wolter Pieters, thank you for pushing me further and providing comments through which I have been able to improve my work. I appreciate the combination of your technical insights and the knowledge of philosophy and sociology that you have.

Without doctoral candidate Pekka Tetri who is the co-writer, co-thinker, co-idea generator, and my source in the world of 'hands on' information security, this dissertation would be very different. It was you and the subject of social engineering that brought us together. Thank you for the memorable journey from ITAIS to JAIS (and BIT)! Talk about becoming! =)

F-piiri – the Foucault reading group (although it is no longer about Foucault since we finished his books!) – has been my academic place of learning, a perfect home for a parasite to make noise and develop thinking. Thus I thank you Docent Seppo Poutanen for always giving me insightful comments whenever I have asked for them. Thank you Docent Ismo Kantola – who could ever have more ideas than you? A man who reads his Foucault in French gets my respect! Dr. Katariina Löfblom, thank you for your thoughts in the group and thanks for teaching me how to conduct interviews properly.

Also, I've always enjoyed our discussions on films. Olli is also part of the group, thank you for that!

Thank you Ph.D. Kai Kimppa. Your support in the very beginning (especially with the first article) was tremendous. In the beginning of my research career Markku Hongisto helped me get my first project research job. Thank you. Thanks go also to Professors Harri Melin and Jani Erola who have made my task easier by employing me. I'd like to thank everyone who has participated in the researcher seminars organised by Sovako and the unit of sociology. I've received a lot of support and always felt welcome. Docent Elina Oinas, thank you for your comments and your support. Assistant Professor Suvi Salmenniemi and Docent Suvi Keskinen, thank you for your support.

I have had the pleasure of spending time at the unit of sociology: it is and has been a place full of many wonderful and beautiful people. Doctoral candidate Carita Lockmer – rock on! \ _ / Dr. Liisa Lähteenmäki, Ph.D. Jutta Ahlbeck, Coordinator Marja Andersson, Docent Päivi Naumanen and the best secretary in the world Jaana Tähti, thank you for always being there for me. I have enjoyed your pleasant company very much. Doctors Arttu Saarinen, Johanna Kallio and Antti Kouvo, thanks for those lunchtimes that we have shared together at that parasitically noisy Macciavelli. Dr. Mari Toivanen and soon to be Dr. Johanna Nurmi, thanks for sharing this experience of 'becoming a doctor' in autumn 2014 – what a ride! Doctoral candidate Ying Liu, thanks for all the sweets you have brought me from Taiwan!

Language is noise. Thus, I'd like to thank Mr. Mark Smith for reading my parasitic texts and getting some sense into them. Also Mr. Adam Ulrich and Master of Social Sciences Laura Kopu, thank you for correcting my language. The mistakes are mine, but without you three the text would be less understandable.

In addition to all my friends with whom I have shared my enthusiasm, joy and despair, I want to thank my family, my mom and dad, and my dear brother Marko – thank you for everything. I have always known that you are there for me – I love you all. Thank you Touko – you're the best! Irene – you're the one, no matter whether it was laughing or crying together, you're the one! Thank you for sharing and mixing your life, thoughts, and love with mine.

Turku, September 23th, 2014

Jukka Vuorinen

LIST OF THE ORIGINAL ARTICLES

I Vuorinen, J. and Tetri, P. (2012) 'The Order Machine - The Ontology of Information Security', *Journal of the Association for Information Systems*, 13(9), pp. 695–713.

II Vuorinen, J. (2013) 'What makes an entity an information security threat?', *An article manuscript*.

III Tetri, P. and Vuorinen, J. (2013) 'Dissecting social engineering', *Behaviour & Information Technology*, 32(10), pp. 1014–1023.

IV Vuorinen, J. (2007) 'Ethical codes in the digital world: comparisons of the proprietary, the open/free and the cracker system', *Ethics and Information Technology*, 9(1), pp. 27–38.

1. INTRODUCTION

Things decay. Everyone knows how organic matter decomposes, decays. A piece of food left in a fridge turns unrecognisable in the course of time. The mixture of grey, green, and blue rhizomes of mould take over. A revolting stench reveals that it is rotting. I should take care of food better. In autumn I love gathering mushrooms, funnel chanterelles, which are, unfortunately, prone to going mouldy very quickly. I do not want mould to come between me and my meal. When chanterelles decay, my meal festers, microorganisms feast, mycelia prevails. In terms of preservation, water in the mushrooms constitutes the issue. How do you stop the rot when moisture summons mould and nurtures bacteria? The rhizome entities – the funnel chanterelles – attract other rhizomatic entities, mould. The moist beginnings of the decaying process can be temporarily halted. I decide to take care of the mushrooms through freezing. The process slows down the process of decaying. I could submerge the mushrooms in vinegar in order to drive out the fresh water within or use salt to do the same trick. Alternatively, I could dry them off in order to exclude the water. The dried mushrooms can be then restored by soaking them in water. First exclude, then include; interrupt and connect in order to avoid disturbing entities, decay. That is also *the logic of information systems and information securing*:[1] format, clear, delete; build walls, scanners, detectors and machines of preservation in order to exclude the undesired elements and then install, implement, use equipment and applications in order to include the desired elements in a certain order. This – how entities (human and non-human), in information security terms, become connected and included through interruptions and exclusion – constitutes the main theme of my research.

The goal of information security is to achieve confidentiality, integrity, and availability for a piece of information, system or service (see e.g. DeKay & Belva 2009, pp.8–9; Bishop 2003, p. 3; Article 1).[2] In this attempt, nothing is allowed to make a connection with the protected system without the control of information security. In terms of confidentiality and integrity, only the authorised entities (for example, particular users and client programs with specific rights) should be able to access (i.e. in terms of confidentiality 'to see particular information') and modify (in order to ensure the requirement of integrity) the protected object. Thus, confidentiality and integrity are based on exclusion, limiting the number of users and programs that can access and modify the object. In simple terms, the undesired (unauthorised) are left outside. However, those who are authorised are included; importantly, this inclusive connection emerges through the exclusion of

1 My intention is to emphasise that information security is always a process. Thus I use 'information securing' and 'information security' synonymously throughout the entire dissertation.

2 The articles that are included in this dissertation are referred to as Article 1, 2, 3, and 4.

the others (the unauthorised).[3] Availability is based on the same pair of inclusion and exclusion: a protected piece of information, system, or service should be accessible (available) for the authorised entities. This means that when a web-based service is down – i.e. not available – it is not secure simply because it is not accessible. However, in terms of granting access privileges – in the process of creating a passage to the system – the term 'availability' does not refer to all-inclusivity in the sense that every entity would be welcome. Rather, the requirement for availability works with confidentiality and is thus also exclusive. As access is made possible (inclusion), the unauthorised entities are nonetheless excluded. The safe and seemingly orderly inside – that is, the system itself including its authorised users – is created through filtering (Article 1).

1.1. Pervasive information security

A sociological approach to information security is needed since we constantly live in and with the overwhelming world of information security. In other words, confidentiality, integrity, and availability are constantly sought. Information securing is overarching and connective: 'Protecting data in electronic format inevitably includes defending all systems, media and communication channels that carry it' (Vladimirov et al. 2010, pp.18–19). In our day-to-day lives, in which our messages are technologically mediated, we are usually immediately connected to information security in the form of entering user names, passwords and pin codes, carrying electronic keys, and using fingerprint scanners. We are all bound to the requirements of confidentiality, integrity, and availability. Even when we are not directly coupled to information securing activities, we are never many steps away from information security. We use products that are directly connected to information security. For example, the movies, music, and computer programs we consume can be copy-protected and even the equipment we use (e.g. HDMI-devices) can have content protection properties. Our monetary transactions – and in fact the entire sphere of trade – are dependent on protected systems. As computing becomes ubiquitous – which here means that devices that carry a program code are no longer sitting on our desks but with us anywhere and everywhere (from cars to ovens, operating theatres and automatic door closers) – information security spreads with the code, since information securing is (or should be) a feature in software development (see e.g. McManus 2009; Gupta et al. 2007). As various electrical devices at home become smarter, they become more and more connected to questions of information security (e.g. Denning et al. 2013). Even cars have information security issues (Wright 2011). In factories, information securing is

3 Essentially, this is to say that the existence of authorised entities implies the existence of unauthorised entities. If information is open and access or visibility desired for everyone – for example in the case of a web-based advertisement – then the requirement for confidentiality is not relevant. Nonetheless, in such a case, there still is authorisation present in terms of integrity: limitations on who is allowed to modify the contents of the information.

needed in order to make production lines reliable. Furthermore, the process of product design takes place in an environment which is full of information security measures. Thus, most products and things, which are in everyday use, have been in a guiding and assisting connection with information security at some point of their creation. With a poor state of information security – for example with flaws in the program code – the products are more likely to have faults.

As gathering data concerning our electronic behaviour (e.g. the tracking of purchases, phone calls, and internet activity) has become easier through the development of technology, we have become entries in a number of registries. The development of more and more e-government projects pushes this further as communication between e-citizen and e-government increases (see e.g. Saha et al. 2010; from the surveillance and privacy point of view see Ogura 2006). Simultaneously, questions about the confidentiality of this communication emerge. Bannister and Connolly (2012, p.211) define e-government 'as the use of ICT in and by governments and public administrations over the period since the adoption by governments of the Internet and the World-Wide-Web in the 1990s'. Furthermore, we are not mere bystanders in relation to information securing as we are – as employees and users, for example – harnessed in the application of information security. Essentially, all organisations apply information security policies – i.e. regulation and rules on how to use information technology devices – thus employees become a part of the machinery that carries out information security (Article 1; Article 2; see also Willison & Warkentin 2013; Siponen & Vance 2010; Bulgurcu et al. 2010). In addition, problems arise when employee-owned mobile devices with various operating systems are used in the working environment (Qing Li & Clark 2013). We also face requirements for being a good user. The question of how to make users obedient (in terms of security awareness) has even been connected to prescriptive – normative – ethics (see Siponen 2000, p.44). More generally, we are told to use security software and strong passwords, not to use the same password for several services (so if one is breached then the others will still stay safe), to keep updating, to be aware of malware, to comply with information security policies, and not to fall for phishing emails.[4] Furthermore, these requirements increase as more devices are introduced. Thus, information security is tightly coupled to many aspects of our everyday life.

1.2. Decay

If a piece of information, an information system, or a service is left without care – without information security, that is – then information and its medium can be taken over by

4 The terminology can be very interesting. For example, 'For password authentication systems, users often *are* the enemy' (Gaw & Felten 2006, p.44), Users are not referred to as 'a problem' or 'a challenge', but rather as 'the enemy'.

outside forces (Article 1) that are comparable to decay. This research uses 'decay' as a general concept referring to the disruptive forces that drive entities to become different. Such forces are, in fact, essential concerns of information security. For example, if an old version of an operating system is installed on a machine which is connected to the internet without a firewall, then the computer will be infected by malicious software and become slower and more unreliable (Arnett & Schmidt 2005). Moreover, confidentiality is lost because malicious software can function as a backdoor program through which information leaks out and which allows outside access to the computer. In the case of an email account (service), almost unstoppable spam (unsolicited email) is an old problem (e.g. Mossoff 2004, pp.631–632). However, from a user's point of view, spam has turned into a less extensive issue because of hard and constant work towards the development of effective countermeasures (Goodman et al. 2007). Nevertheless, if spam is not gotten rid of, then one's inbox will become full of uninvited email messages. In a messy inbox, spam is noise, disturbing decay, which comes between the reader and desired emails. Just as the infected computer requires extra time to run the malicious processes (Arnett & Schmidt 2005), a mail user requires extra time to sort the desired messages from spam. Interruptive decay – here spam and malicious code – stems from the outside, weakening the availability of the information, system, or service.[5]

In addition to intrusive and interrupting spam and malicious software, the digital world is filled with different kinds of decay: forces that interrupt, break in, are excessive and useless, and modify structure without authorisation.[6] Thus there is plenty to exclude in preserving information security. In information systems jargon, there are even some examples that resonate at the semantic level with the notion of organic decay. For example, 'link rot' refers to a dead link that leads nowhere other than a 'not found' error page (cf. Bugeja & Dimitrova 2010, p.28). Here as well, decay or 'rot' is in fact about interruption, in the sense that the link is cut off because the referent page does not exist anymore. 'Software rot' and 'bit decay' emerge when the utility of a code is lost because the ideas behind the code are not spelled out and made available to others by the creator(s) of the code (Lougee-Heimer 2003, p.58). In other words, a code that is left without connective care – in this case, documentation – will be lost. Written documents about the code would carry the code forward, mediate it: documentation would be taking care of availability, continuity. 'Bit rot' is, however, an even broader phenomenon than non-documented ideas relating to the development of code. 'Bit rot' also refers to data that is lost when different digital formats (whether devices

5 The division between inside and outside is conceptually important to this research. Whereas the inside is a controlled region (or is sought to be controlled and organised in terms of forces), the outside is out of control, the space of decay. The two concepts are examined more closely in Section 4.2, 'Outside and inside', and in Article 1.

6 For more on 'the dark side of digital culture' see Parikka and Sampson (2009).

or software) are no longer supported (Weinstein 1999; see also Truitt 2009).[7] At the time when I was working on Article 4 (which, chronologically, is the first article), a CD-ROM was still a viable, albeit declining, medium for the distribution of programs, but now the situation is entirely different. As a mass storage medium, the usability of the format has deteriorated since more agile (and relatively cheap) options, namely flash drives and cloud storage services, have become available.[8] The decreasing number of players is a crucial part of format decay. Thus the environment in which the format is used takes part in the process of decay.

Decaying is about becoming different in such a way that the decayed object can no longer be utilised in or by its old connections because the connections are interrupted by decay. Therefore, a CD cannot work as an effective distribution medium in an environment in which there are not enough players to connect with. The format decays. Decay is interruption from outside. It is a process in which an alternative order invades an entity or its connections. A decaying mushroom does not disappear but it transforms; it is replaced by a set of connections. After a notable mould interruption, I cannot use the mushroom as a source of energy in a convenient manner – without getting food poisoning, that is. Normally, I cannot 'communicate' with mould directly. However, here the mushroom provides a medium – a source of energy for us both, me and the mould – and through the mushroom we can fight over the territory, the mushroom. The mushroom is a connective passage between me and the mould. The question is which one will be excluded. In terms of information security and in the case of information and the requirement for confidentiality, integrity, and availability, the question is very similar: who is authorised to access and modify, and who is excluded? Put simply, 'who is the user?' The integrity of information, its order and organisation on a medium (see Article 1), can be broken, as can the structure of a funnel chanterelle. When information is broken down it cannot be used; availability disappears with usability. With decay, entities are excluded – but also connected. I cannot communicate with malware directly but through an information system the communication is possible. The argument that 'things decay' invites the question 'who is interrupted?'

7 'Bit rot' can refer also 'to the [physical] decay over time of digital storage media whereby digital data is corrupted at the level of individual bits' (Cothey 2010, p.222).

8 This situation is not new. Using a floppy disk would be frustrating in the current environment. Decay concerns analogue data and its formats as well. I have a pile of VHS tapes decaying in the attic and no device through which to convert the tapes into another format. Thus, in the attic, old MacGyver episodes are dying alongside Dempsey and Makepeace – what a loss. With two VCRs I could produce copies of the tapes but each copy generation comes with increased noise and finally there would be nothing but noise (see http://www.youtube.com/watch?v=mES3CHEnVyI).

1.3. The structure and approach

Considering how closely intertwined information securing is with our everyday life, it is a relevant subject to study. For me, it is interesting to examine how a piece of information can be broken by entities that are considered malicious and, furthermore, how these entities interrupt activities, and transform sets of connections around information systems (Articles 3 and 4). For example, removal of a copy protection system, which is an element of information securing, breaks the connection between control and copies; the order in which copies have a controlled source, becomes different as control over sources is lost (Article 4). In addition, it is interesting to examine in what a way an entity becomes a threat (Article 2, implicitly in Articles 3 and 4). These issues relate to what I have called here 'decay', that is, disconnecting, breaking down, breaking in, exclusion – essentially interruption. Again, I emphasise that decay produces mutation and provides a new organisation, a new set of relations. In this sense decay is creative and productive. However, although decay – in the sense of the rupturing forces from outside – is interesting, the countermeasures, which seek to hold things together and stop the decay by building different kinds of walls, fascinate me more. Hitherto, these walls have largely been examined in terms of practical development, in order to learn how they could be made and designed in sturdier ways so that a higher level of security could be achieved (see e.g. Siponen et al. 2006; Bulgurcu et al. 2010; Siponen & Vance 2010). Instead of focusing on such aspects of practical improvement, *in my research I want to create concepts through which we can examine information security itself as an actor beyond its role as a protector.* In fact, I argue that information securing in itself is an interruptive force (Article 1). Importantly, it interrupts both the forces of the inside (for example employees and equipment) and the forces of the outside (for example malicious software or network traffic). A computer requires an immediate reboot in order to install critical security updates.[9] Is that not an interruption of a protected region? Old fashioned DVD movies display a copyright announcement when the disc is inserted. In other words, information securing interrupts in order to produce a secure state. To rephrase my approach using terms related to the example of the mushrooms, I am not studying how much vinegar is optimally needed to preserve a certain quantity of mushrooms – how to prevent decay – but I want to focus on what happens to the mushrooms in the sour state caused when they are preserved, soaked in vinegar this way: how do the mushrooms taste? What kind of cooking does the vinegar make possible? Furthermore, I want to examine whether it is possible to use vinegar for other purposes than preservation, to shift from exclusion of decay to inclusion of taste. In other words, information securing is much more than making information, systems, and services secure. It is a producer, connector, and interrupter.

9 Furthermore, patching does not necessarily make the computer secure (Gardner, Bishop and Kohno 2009).

This dissertation consists of four articles and this 'Introduction'. I examine what information security is (Article 1) and how an entity becomes a threat (Article 2). Article 3 focuses on examining how 'social engineering' – this refers here to ways of breaking into a technical system by 'social' means – is studied, and extrapolates a new framework. Article 4 studies groups that remove copy protection from software and then distribute the software for free. In this 'Introduction', I explicate the connections between articles, and seek to summarise and underline the results of the study. However, this part does not replace the articles. The ideas are developed and unfolded in the articles in more detail. I link the articles here by summarising and developing further the main concepts that are scattered throughout the articles. In the simplest terms, I examine the question of who is interrupted and where the interruption comes from, in terms of information security.

This is a story about the entanglements of interruptions, from decaying mushrooms, noise and din to cracked copy protection and 'socially' invaded information systems. This is an examination of order preserved, security broken, the allure of fame, storing and restoring, signing, and property. Finally, this is a description of the emergence of alternative orders, connecting channels, leftovers, and interfering parasites. Ultimately, it is story of difference and becoming different, transformation: how an entity is transformed through interruption, how reorganisation creates relations.

I start with a brief introduction to the articles and discuss what they are about. This is followed by a brief explication of my theoretical position and an account of the methodology. In addition, I spell out what 'ontology' means in terms of this research. Then I move on to the key concepts of the study. The concepts of noise, order, outside, inside, machine, actor, the order of users, parasite, and subjection are examined, along with some related concepts (such as interruption and territory). These concepts relate to what information security is, how systems function on difference, and moreover how information security has to deal with that difference – whether in the form of security threats or normal use. After the key concepts section, I fold this study in on itself as I return to the articles about software crackers and social engineers in light of the concepts explored. Finally I go through the conclusions of the entire study.

2. A QUICK LOOK AT THE ARTICLES

Initially this study stems from my interest in software crackers. The crackers form groups that remove (i.e. crack) software copy protection and then release the programs for free. Although I commenced with an examination of the world of cracking and found it quite intriguing, the fundamental questions relating to information security began to grow in importance over the course of my research. Thus, in Article 1 (which is in fact chronologically the second to have been written) 'The Order Machine – The Ontology of Information Security', I examine *what information security is by what it does*. In the article, information security is described as an interruptive and connective machine that seeks to purify its territories by excluding all the impurities in order to preserve order, that is, the confidentiality, integrity and availability of information, information systems and services. In this way, pure insides are generated: thick border – controls such as firewalls, password enquiries, and encryption algorithms – lie in between the orderly inside and the chaotic outside. However, an inside – such as a computer, a user account, a mobile phone system or simply an information system – is never free from impurities as everything the inside is made of originates from outside. In other words, the inside is always a fold of the outside. Although the aim is always to organise and purify the inside, some potentially chaotic and disorderly elements can survive purification. Furthermore, the interesting point is that as the territories are purified, information security – through activity relating to it – becomes the *third* entity that interrupts the relation between the system and the user. For example, as I wrote this text, I was interrupted by a client security program's version update request to restart the machine. In other words, information security excludes interrupters such as malware and network intruders, but it is in itself a similar interrupter as, for example, updates and reboots are required to keep the system in order. In summary, information security is based on interruption but it interrupts entities whether they are within or attempting to enter the system from outside.

But what are the impurities that the constantly changing security assemblage (the heterogeneous actors of information security which are connected to each other) seeks to exclude? It could be argued that the 'impurities' refer to malicious entities (e.g. malware). However, this is not in fact a proper answer to the question but rather a mere rephrasing of that question, as it could then be asked, what makes an entity 'malicious'. Thus it is relevant to ask what makes an entity an information security threat. This question is explicitly examined in the second article, which carries the question as its title: 'What makes an entity an information security threat?' An entity is never a threat in its own right. First there has to be a system to which the entity poses a threat. A single entity is rarely a threat to all systems. For example, natural disasters are always more or less local; they never pose a threat to every system that exists. The system and entity should share

a common passage. This pertains to the ontological theme of the first article: the chaos outside is never *total* chaos, which would mean that it was entirely incomprehensible in the system's terms. If something can be apprehended as chaos, then there has to be some sort of understandable form. Otherwise, chaos could not even be understood as an actor and it could not be communicated with. For example, a Windows-based virus cannot hurt machines running Linux; such a virus does not have a passage to Linux. In fact, a Windows virus can be examined within a Linux-based system but the virus cannot act. It cannot multiply or, simply, it cannot use the system. However, a tsunami – a threat entity of its own kind – treats Windows and Linux machines equally. Most importantly, in order to constitute a threat, an entity's logic of use (the effects it causes on the system) is required to be in contradiction with the purpose – or logic – that is imposed on the system by its (original) user.[10] If the entity's logic of use does not contradict the original user's logic of use, then it is a case of mere use. For example, I do not want an outsider to read my emails (this is my logic of use). However, I need to use a client program to enter the mail server and retrieve my emails. In a sense, the program is an outsider but I allow it to access my mail. In other words, it does not contradict my logic of use but in fact helps me to carry out my logic of use – that is, reading my emails. However, if there was some vulnerability in the client, a flaw that would allow an outsider access to my emails, then the combination of the client, the server, the outsider and my logic of use would constitute a threat, not separately but together. In terms of threat, the logic of use matters. Moreover, the logic is imposed on the system – or on an assemblage or a machine (Article 1) – as the system is used. Furthermore, when the system is used, the system is harnessed to serve the logic. There is abuse before use (Serres 2007, p.7). In short, systems themselves do not have a purpose, but an inner logic, a way of functioning – 'an order' as argued in Article 1. But when the system is used, it means that it is harnessed to serve an external logic: the system is coupled to serve the other.

Article 3 (Dissecting Social Engineering) is about social engineering, which is a general term used to describe all non-technical means that are utilised in information system intrusions.[11] For example, to gain access to someone's account simply by directly asking for their password to the account would be a case of social engineering. Finding valuable information in a dumpster is another example. SE can be divided into three dimensions: persuasion, data gathering, and fabrication. In an attack all the dimension can be present with different intensities. Persuasion refers to an attempt 'to get a person to comply with an inappropriate request: to make them do something which is against the rules or a set of norms (e.g. an information security policy)' (Article 3, p.1016). The dimension of data gathering refers to the techniques of attack through which valuable information

10 With 'logic' I refer to the way in which a system functions, possibly including the purpose of use.

11 In other words, in my work the term 'social engineering' is not used in the political science sense (i.e. trying to solve social issues by influencing particular groups in society).

(valuable in itself or in terms of the attack) is acquired. In practice this can mean going through the rubbish, taking photographs, or talking to employees in order to get project names, for example. Fabrication, on the other hand, refers to the manipulation of the victim's interpretation of the situation. In other words, the intruder plays an appropriate role to get the desired object or information. For example, playing the role of a regular customer on the phone with a stolen social security number can make an intrusion into an information system possible. In such a case the victim of the fabrication might be a customer service representative.

The main argument of the article claims that in research on social engineering the dimension of persuasion has attracted most of the attention. Moreover, seeing social engineering as mere persuasion leads to a biased understanding, in which the dupe's (victim's) role as a weak personality (a weak individual who falls so easily for persuasion) and the intruder's skills are overemphasised. Thus, social engineering is seen as a set of mythical skills with which the social engineer makes people do things they would not normally do. However, the dimension of fabrication – which establishes the intrusion based on the dupe's interpretation of the situation instead of targeting the dupe's personal characteristics – is, in terms of logic of use, mere use of the system. To continue the examination of the aforementioned example of an intruder with a stolen identity calling customer services, we can observe that the customer service representative is not persuaded to do anything inappropriate but is in fact carrying out their normal job. It can be argued that the intruder merely *uses* customer services. However, the intruder's logic of use is in contradiction with the logic of use of the organisation. Simply put, the social engineer invents a new logic for customer services, imposes his or her logic on it, and plays the role of a customer in order to get the desired information.

Article 4 (which, chronologically, is the first article), 'Ethical codes in the digital world: comparisons of the proprietary, the open/free and the cracker system', deals with the software cracker groups that have invented a new logic for copy protection systems. The proprietary software producers use copy protection to prevent (or interrupt) free distribution of their property, an application. The cracker groups, on the other hand, invent a new logic for copy protection systems as they compete in breaking the systems and releasing the cracked programs. The competition that goes on is a peculiar one – I call it the prestige or honour game. The game is about which group releases the cracked program fastest and in the most reliable manner. Thus even unreleased proprietary programs can be available because of these cracker groups' activity. In relation to copy protection, the logic of proprietary software producers clashes with the crackers' logic of use. However, the logics of the two are similar in terms of freezing the products in a certain form: proprietary software producers try to freeze their products in the form of an artefact. By this I mean that through copy protection the product has a single,

unique source: it cannot be copied even though it is in digital form. In simple terms, control stays with the producer. In that sense the product is frozen. However, the prestige game is fuelled by copying. The cracked copies of programs spread out and in return prestige, honour and respect flows back. In order to enable the crackers' prestige game, rules are required for the game. The groups' releases – cracked programs – are signed with the name of group that has cracked and released the program. The honour code of the cracker scene requires that the signature cannot be changed by other groups. For example, if a group released a program that was cracked by another group, the group which 'stole' the release in this way would be excluded from the scene. Hence the cracked programs are still property; they are the property of the cracker group. Again the object is frozen. It cannot be freely modified. In the article, I suggest that free software movement provides another kind of paradigm in which the program is not frozen in any manner.

The first and the second article are tightly bound together through the examination of information security and information security threat. In a sense the two are siblings, as the first article deals with the order machine and the second is about the emergence of threats to a machine. The third and fourth articles deal with two different cases relating to information security. In social engineering the emphasis is on the manner in which the intrusion is made. As the techniques and their dimensions of intrusion are extrapolated, fabrication stands out as the most interesting dimension. In terms of this study, fabrication is intriguing because in fabrication information security is coupled as a part of the intrusion. In fabrication, information security policy generates the passage to the system for the intruder. I explain this in detail later (in Section 5). In Article 4, information security comes in the form of copy protection, and crackers are the threat to it. Instead of paying attention to the techniques of cracking, this article treats copy protection – in the terms used throughout this dissertation – as an example of how information security provides a playground for the crackers, and makes their game possible. Here information security is an enabler in its attempt to interrupt. Furthermore, the crackers have their own way of creating copy protection: signatures which are protected by the collective and through which the products (the releases) are made the property of a particular group. The crackers, however, also face their own threats that pertain to breaking the rules of the honour game. Articles 3 and 4 describe an alternative way of harnessing (see Article 2) information security (see Article 1) for another activity; an alternative logic is imposed on information security. In short, the harnesser becomes harnessed – (ab)used.

3. NOTES ON THEORETICAL BACKGROUND AND METHODOLOGY

3.1. The three fields

In terms of theory, my research has been divided into three different fields. On the one hand, my home field has been *sociology*, from which I have regularly taken journeys into the field of *philosophy*. On the other hand, *information systems science* has provided the main theme of this research, namely information security. It is as if I had stood in a field next door to information systems science and constantly gazed into the neighbouring field, looking at their problematisations, contemplating their conceptualisations, and observing their questions, and then sought to figure out what kind of sociological questions – still relevant to information systems science – could be posed about the neighbouring field's buzzing topic of information security. In addition to taking the theme from a field other than my own, I have drawn elements from philosophy – for example Deleuze and Guattari's (1983) concept of 'machine' and Michel Serres's (2007) concept of 'parasite' – in order to make my sociology theoretically sturdier. In other words, I have observed one field and absorbed thoughts from the other. There I stand in the field of sociology bringing the two other fields together and making them all connect. The fruits of my research – my contribution, that is – can be embraced in all three fields. Yet the main contribution goes to information systems science and sociology.[12]

Nevertheless, I have made my first shortcut here by implying that the three fields are somehow separate from each other. In fact, the divisions between the fields are not that sharp and clear-cut; rather the fields overlap or are intertwined. Furthermore, there is a messy order within the fields as well. When it comes to my home discipline, there is no single 'sociology' but many 'sociologies'. Thus, I would like to spell out which sociology I refer to – in other words, what my sociology is. Bruno Latour (2005, pp.5, 12) distinguishes between 'sociology of the social' and 'sociology of associations'. The former designates the major body of sociology springing from Émile Durkheim (Latour 2005, pp.23–25). The latter, on the other hand, points quite directly to actor-network theory (ANT), an approach developed at the *Centre de Sociologie de l'Innovation* in Paris by Latour, Michel Callon and John Law in the early 1980s. At first ANT focused solely on conducting research on technology and science. More recently, the scope has expanded to cover other topics and questions as well. (Latour 2005, pp.10–11.) Latour finds a number of differences between the two schools. For example, ANT is based on

12 This resembles the way that philosopher Elizabeth Grosz (2001) contributes to the field of architecture by examining architecture from the perspective of Continental philosophy.

the thought that stability – of a group for example – is always the result of constant work and effort rather than being a natural state of affairs, whereas sociology of the social tends to take stability for granted. Thus, for sociology of the social, decay and conflicts are exceptional cases which need to be explained. ANT, on the other hand, considers that stability has to be explained. (Latour 2005, p.35.) In other words, ANT emphasises change and transformation and thus prefers to consider society (or a collective [see Latour 1999, pp.193–202]) as a process rather than a stable structure. However, Latour (2005, p.70) points out that it is the approach to the agency of (non-human or) material objects that makes the decisive difference between the two schools. ANT embraces heterogeneous actors: human and non-human (Latour 2005, pp.70–72; 1999, chap.6). In fact, material objects participate in our daily lives in such a manner that we could not survive without matter. ANT emphasises that material objects mediate and keep up our social connections. Sociology of the social emphasises invisible and coercive social forces instead (Latour 2005, p.21). In ANT, the 'social' leaves traces; it is in events of connecting; the social is a connection, an association, a coming together; it is '*with*' and there is always matter involved (Pyyhtinen 2009). The agency of an actor is thus not in an individual point (initiated by an intentional consciousness for example); agency is dislocated. It is dispersed and shared through connections. (Latour 2005, pp.46–47; see also 1993, pp.117–120.) Action is collective and mediated. For example, I write this with a computer; I do not write *solely* by myself but *with* the computer (cf. Dant 2004; Latour 1999, p.193). However, it is not as if the computer could write by itself, but rather it is a significant part of the writing process which also transforms the process of writing (see Latour 2005, p.71; also Introna 2011). As an actor the computer can connect me with a dictionary, and make printing and emailing possible. Nonetheless, the connection between me and the computer is not important in itself. What are important are the *emergent properties* – the ability to act differently – which emerge with the connection (Latour 1999, pp.179, 182–183; Bennett 2010, p.22). For example, I write and edit more quickly with a computer than with a quill.

In terms of my research I have adopted the idea of non-human actors and the concept of emergence (see Article 1; Article 2, also Article 3, p.1016). I use the term 'assemblage' to refer to these heterogeneous actors working together (see Bennett 2010, pp.23–24; also Latour 2005; cf. DeLanda 2006). In addition, I share Latour's emphasis on 'processes' (e.g. 'becoming' in Article 1) and overall the relationalist approach to dislocated agency and how things become significant only through their emerging relations (see Article 2 and how an entity becomes an information security threat only in a certain set of relations). Although I draw influences from ANT, I do not however consider my work as an ANT study as such, since I have not traced and analysed empirical actor networks. Rather, in terms of methodology, my work is based on theorising. As a method, theorising or thinking are not straightforward processes. Colebrook (2002, p.38.) aptly writes in the

Deleuzian manner that 'Thinking, […] is not something that we can define once and for all; it is a power of becoming *and* its becoming can be transformed by what is not thinking's own – the outside or the unthought. Thinking is not something "we" do; thinking happens to us, from without. There is a *necessity* to thinking, for the event of thought lies beyond the autonomy of choice. Thinking happens.' In other words, my work is more abstraction than the tracing of networks. It is the construction of concepts and the creation of connections between the concepts rather than observing an empirical sphere. I have observed thoughts, logics (how things work), and concepts more than the empirical field of things and events.

In other words, instead of fully being a Latourian, I rather go straight to his sources of inspiration. Latour has been greatly influenced by his teacher Michel Serres, a French philosopher with a diverse range of themes, from the philosophy of science to communications and social theory. Latour has harnessed – or translated – Serres's thinking to serve empirical research.[13] Since this has been one of Latour's main contributions and as my emphasis lies in theory rather than empirical data, it has been tempting for me to draw directly from Serres. Serres's ideas are fuzzier, more imaginative and less strictly outlined than Latour's. Thus, I welcome Serres's style because it fits my purposes perfectly: the raw concepts leave more room for transformation and creation. The Serresian concepts – such as the 'parasite' or 'noise' – are not complete but open (see e.g. Serres 1995; 2007). From Serres (2007, p.19) I have taken the idea of the third (the parasite): if two things can be considered as a pair then there is always something, the third (the parasite), in between the two. That third is always inclusive (connective) and exclusive (Serres 2007, pp.22–25, 241–242). This thought is utilised in Articles 1 and 2. In addition, it is implicitly present in Article 3.

If Serres's ideas are open, the same openness applies to my other source of philosophical influence: the two French philosophers Gilles Deleuze and Félix Guattari.[14] For me, Deleuze and Guattari (1983; 1987) are mainly inspirational sources, which means that I have taken some of their concepts ('machine' and 'rhizome'; the latter is quite implicit in my work, and territorial thinking and interruption springs from them but also from Serres [2007]) and put them in a new environment and made them work for me. In fact, this is quite the Deleuze-Guattarian way to use concepts (Deleuze & Guattari 1994; see also Grosz 2001; 2008). However, I do not claim that I am conducting research on Deleuze here.

13 For example, Serres's (2007, pp.224–234) concept of quasi-object has been adopted by Latour(1993). In addition, the idea of mediation and translation (Latour 1993, pp.11, 79–82) is included in Serres's (2007) concept of 'parasite.'

14 Latour (1996) has drawn quite extensively from Deleuze (and Guatttari) as well.

Latour is not the only sociologist that I use. Niklas Luhmann, a German sociologist and system theorist, has been a great aid in systemic thinking. In particular, his analysis on the relation between a system and its environment has been drawn upon in Article 2. In Article 4, I use Luhmann's (1989, chap.8) concept of 'code', through which I seek to analyse differences between the three groups (software crackers, the open/free software movement and proprietary software producers). Whereas Latour removes the human-centred perspective from the heart of sociology by considering non-humans as actors, Luhmann (1989; 1995) replaces the human-centric approach with one focused solely on communication. It is communication – the circulation of messages – that matters, not individuals as such, because it is communication that produces the system, not the individual message carriers. Latour and Luhmann's conceptualisations of sociology can be used together (e.g. Teubner 2006). However, from my point of view, Luhmann fails to grasp the significance of materiality in the social. Furthermore, the Luhmannian systems are too clear cut – there is no fluid blending, but purified lines of systems and codes (e.g. Latour 2010, p. 263). Thus, I use Luhmann more as an inspirational system theorist than a provider of entire ontology (I discuss ontology thoroughly in the following section). While Serres addresses communication as well, he emphasises materiality in the social (e.g. Serres 2007, pp. 224–234).

The influence of Michel Foucault (1985), a French philosopher and social theorist, is obvious in Article 4 (in the analysis of ethical codes) and is implicitly present throughout the work. Foucault's (1978; 1982; 1995) concept of power is utilised in Article 1 although the reference in the article is a mere footnote. However, a two-way power relation is obvious in the concept of 'subjection' (Article 1 and see also Section 4.7). In addition, Foucault (1994; 2002) describes a system of statements, discourses, and epistemes that, as an approach, has influenced me tremendously. Foucault (1994, p. 155) is another name in the list of researchers who set individual human subjects aside and examines what is actually said.

The connection between information systems science research and philosophy is not new, as most theories are usually rooted in philosophy.[15] There has been vibrant discussion about the significance of theory in the field of information systems science (e.g. Lyytinen & King 2004; Lyytinen & King 2006; Weber 2012). Furthermore, there has been debate over the connections between this field and other disciplines, with questions arising over the identity, differentiation and independence of information systems science (Baskerville & Myers 2002; Gill & Bhattacherjee 2009). The strongest bond between information security research and 'sociology' resides in the interest in human behaviour. For example, one such question is that of why employees break rules

15 Conventionally, 'information' has provided a subject for philosophers but information system scientists have also problematised the concept of 'information' (McKinney Jr. & Yoos II 2010).

when using computers (e.g. Willison & Warkentin 2013; Bulgurcu et al. 2010; Qing Hu et al. 2011; Siponen & Vance 2010). However, all research concerning information security in the field of information systems sciences has always contained the normative aspect of improvement: how the systems could be made more secure. In my research, I want to examine information security in itself: 'what it is by what it does' (Article 1), 'what are the requirements for the emergence of an information security threat' (Article 2), and then 'how information security policy can make an intrusion possible' (Article 3), 'how digital information is frozen into artefact form through copy protection systems' (Article 4). All in all, I examine the diversity of information security as an actor. This contributes to sociology and information systems science by pointing out *how* information (systems) security could be researched, and how diverse an actor it is. Furthermore, information security can be harnessed to something completely different (Article 3 and 4). In other words, this examination requires the use of a different type of ontology than that which has hitherto been used in the field of information security. In the following, I expand upon the ontological aspect of my study.

3.2. Ontologies

The term 'ontology' can have different meanings. Firstly, within the field of information system science the term mainly refers to 'an engineering artifact, constituted by a specific vocabulary used to describe a certain reality, plus a set of explicit assumptions regarding the intended meaning of the vocabulary words' (Guarino 1998, p. 4; see also Fonseca 2007). For example, ontology of an information system can refer to the terms that describe the elements (entities) of a system as well as articulating what those terms mean. With its directional way of representing, it could be considered a 'map' of an information system, accompanied by an explanation of the map legend. Secondly, the term can be employed to designate philosophical ontology which relates to the questions of being and entities (Guarino 1998, p. 4). In this study, the term 'ontology' is used solely in its philosophical sense unless otherwise noted. Manuel DeLanda (2005, p. 4) remarks, 'A philosopher's ontology is the set of entities he or she assumes to exist in reality, the type of entities he or she is committed to assert actually exist'. Moreover, ontology (in its philosophical sense) is not exclusive to the field of philosophy; every field of study contains ontological presuppositions. For example, the concept of 'computer misuse' (see Willison & Warkentin 2013) – slightly simplified – presupposes that there are not only entities such as users and computers, but also rules or norms that regulate the use of computers. Furthermore, there is the ontological assumption that computers can be affected by users, and that there is a relation between rules, users, and computers. For information security research, then, the problem that remains to be solved is *how* to affect users in order to prevent misuse. In other words, the question

is, which security mechanisms should be implemented in order to address the problem of misuse in the best possible manner? In information security research, the presence of philosophical ontology is more likely to be implicit than explicit. I will return to this later.

Of course, my use of ontology in the philosophical sense of the term does not yet reveal much about the content of my ontology, since there are a number of different ontologies in the field of philosophy. One way to organise ontologies is to divide them between 'ontologies of being' and 'ontologies of becoming'. This division can be established by asking how ontology approaches 'being'. In simple terms, ontologies of being presuppose that entities remain the same, whereas ontologies of becoming assume that entities mutate, change, and transform. In fact, the differences between ontologies of being and ontologies of becoming quite thoroughly mirror the differences between sociology of social and sociology of associations which were dealt with above. Because information securing is a process in itself, and because the environment of information securing changes constantly, I affirm that 'ontology of becoming' is better suited to use in the field of information security than 'ontology of being'.

I begin the examination of ontologies with ontology of being, which I argue to be the dominant type of ontology in the field of information system science, especially in information security research. In ontology of being, an entity has a fixed identity that stems from the *essence* of an entity (DeLanda 2006, p. 26). There are various versions of ontologies of being, but Plato's ontology can serve as an example because it is well known and relatively easy to grasp in outline. In *The Republic,* Plato (1998) argues that we cannot perceive entities in the way they truly and fundamentally are because their real existence is only revealed at the level of *ideas* (or forms).[16] In Plato's (1998, pp. 193–198) famous cave allegory, our perception of objects is compared to seeing mere shadows on the wall of a dim cave. The shadows on the wall are cast by the light of a fire that is behind people who cannot see each other directly, but only as shadows on the wall. The reality – the level of ideas and forms – resides outside the cave in the bright sunlight. At the level of ideas, we would be able to perceive how the entities truly are, to see what people and objects are really like. Following the allegory further, there are no hazy shadows outside the cave – at the level of ideas – but clear facial expression, blinking eyes, and subtle smiles which would be imperceptible in the shadowy images. However, seeing in clear, bright daylight is not easy since our eyes are used to the darkness of the cave. Plato (1998, p. 198) argues that we need philosophy in order to grasp ideas in their dazzling brightness. In other words, philosophy is the way to the truth – the path to the real knowledge of things.

16 It should be noted that Plato never mentions 'ontology'. The term is an invention of later ages. Furthermore, Plato does not use the word 'essence', this is Aristotle's term. However, Plato's idea can be understood in the same way as 'essence' since it is the foundation of what an entity truly and fundamentally is.

In Plato's ontology, ideas are eternal and perfect; ideas do not transform, change, mutate, or decay. However, entities – for example, the things we see – are imperfect copies of ideas full of errors and variance. Regardless of the discrepancy between an idea and an entity, the entity remains recognisable – identifiable – because of its *essence*. In terms of Plato, recognisability springs from ideas which are the anchors of entities' identities. Generally, ontologies of being are based on the *essence* from which the identity of an entity derives; the variance of entities is limited by common stabile properties. An entity can change on the surface, but according to ontologies of being, it does not change fundamentally. So when I clip my fingernails my appearance changes, but I stay the same person because I was not able to alter my 'essence'. Essence is constant and provides the source of fixed identity (DeLanda 2006, chap. 2).

In ontologies of becoming, there are no essences or permanent properties that would anchor the entities in fixed positions.[17] If Plato provides an example of fundamental ontology of being, A.N. Whitehead is the ultimate philosopher of ontology of becoming. Although Whitehead's philosophy eludes summarisation, I still seek to use it as *an example of (ontology of) becoming* because he places more significance on the concept of becoming than any other philosopher. In Whitehead's view, everything becomes. In order to make Whitehead's philosophy understandable, an introduction to a set of its concepts (which are entangled with each other) would be required (see e.g. Shaviro 2009; Halewood 2011; Poutanen 2013). However, since an introduction of this kind is not possible here, I shall defy the complexity of the concept and try to make sense of Whitehead's becoming through the use of a brief example. Whitehead (2006, pp. 164–168) writes about 'Cleopatra's needle', which is an ancient obelisk transported from Egypt to the bank of the Thames in London. Even though the obelisk seems to be stable and remain the same (as it *is* an obelisk that has been in Egypt), Whitehead insists that the needle is an event. 'If we define the Needle in a sufficiently abstract manner we can say that it never changes. But a physicist who looks on that part of the life of nature as a dance of electrons, will tell you that daily it has lost some molecules and gained others, and even the plain man can see that it gets dirtier and is occasionally washed. Thus the question of change in the Needle is a mere matter of definition. The more abstract your definition, the more permanent the Needle' (Whitehead 2006, p. 167).

However, becoming is not limited to 'physical' change. For Whitehead, entities *prehend* each other. To simplify, they are constituted by their surroundings while, at the same time, they mutually constitute their surroundings. (Whitehead 1978, p. 19.) For example, as I write this text I prehend the light that is emitted by the display. I prehend the sounds I hear and the chair I sit on. I *feel* them and they become a part of my experience; I prehend, I become. (See Shaviro 2009, pp. 28–29; Halewood 2011, pp. 29–32.) In fact, the

17 At least this is true in the case of my research and ontology of becoming that I employ.

text changes me; I am not the same after writing it. Furthermore, it speaks back to me as I read, and I correct and modify it. When my surroundings change, I change as well. This is not that surprising. However, Whiteheadian philosophy argues that the computer '*feels*' me as well: it can 'feel' my use of it and thus it prehends me. Therefore, I am an element in the becoming of the computer. I can see the text on the display – it becomes. Whitehead's conception of the subject can be elucidated by contrasting it to that of Kant. Whereas in Kantian phenomenology the world is the product of a subject, in Whitehead's philosophy a subject is the product of the world (Shaviro 2009, p. 20).

Ontologies of being emphasise the internal relations of entity (see DeLanda 2006, p. 9). For example, when Plato's ideas – or essences – are emphasised, the ideas do not refer to other entities in any manner, they only designate the inner (or transcendental) qualities of entity. Thinking through '*prehension*' serves as an enlightening example of putting emphasis on the external relations of entity. Not only does it question and shatter the stability of identities – yes, I do become different as I clip my nails – it also threatens both the stability of boundaries and the assumed location of agency. There are at least three agents that make nail clipping possible: 'I', the clippers, and the nail. The nail possesses a structure that allows it to be clipped by the nail clippers. If my nails were metal, then the ordinary clippers would not do. Breaking each of the agents down into even smaller components reveals that the totality of an entity is in fact a coming together of many smaller actors: my heart pumps blood (full of cells) which transfers oxygen to my muscles and enables me to clip my nails (in order to simplify, I leave out the possibility of anaerobic muscle movement). (See Article 1, cf. ANT above.) Because the constitution of entities is affected by their external relations, their agency – capacity to act – is dislocated.

In addition to my sympathy for Whitehead's 'prehension', I apply an ontology of becoming that is mainly drawn from Deleuze (and Guattari), and which is, from time to time, very Whiteheadian (see e.g. Deleuze 2006, pp. 86–93).[18] For Deleuze, entities are constantly affected by a field of different forces. Moreover, entities themselves are also affective forces in the same field. (Colebrook 2002; 2006, pp. 1–8; DeLanda 2006; Grosz 2008.) For example, a file on a disk is a force – it occupies space (see Article 1). In addition, it can be the object of different processes such as copying, modifying, and deleting, which are matters of information securing. In the case that the file is a part of an operating system, it produces emergent properties for the computer and the user of that computer (see Articles 1 and 2). In ontologies of becoming, entities are not solitary units (cf. 'Hegelian totalities' in DeLanda 2006, chap. 1); they are also constituted by the connections they have with other entities (in addition to 'prehension' above, see concept of 'machine' in Section 4.3). Entities receive their identity in dynamical processes (DeLanda 2005, pp.

18 In fact, Deleuze creates 'a series of ontologies' (May 2005, p. 16), which makes his ontology easier to employ than that of Whitehead. Deleuze is more agile in this manner.

5, 38–39; 2006, p. 28). This line of thought brings us back to Latour and his emphasis on emergent properties: actors gain themselves and give others new properties through connections (explicitly Article 1, Article 2, more implicitly Article 3 and Article 4). For me, the becoming of entities arises from emerging connections and disconnections (Article 1, Article 2, Article 3, Article 4). Thus, as the connections of an entity change, such as when a copy protection system is removed from the proprietary software environment, new logics and novel ways of use emerge around it: the copy-protection system has become an object in the cracking game (Article 4). In other words, the copy-protection system becomes a different entity.[19] To put this in Deleuze & Guattari's (1987) terms, the copy-protection system has become part of a different *assemblage* (which imposes a new identity upon it) (see Article 2, Article 4, Section 5 in this 'Introduction').

Difference forms the central feature of Deleuze's (2004) ontology. Deleuze is not interested in the *difference* that serves the tasks of comparison and the search for the origin of entity (that would be the essence) (Deleuze 2004; see also 1995, p. 121). For him, the difference – in itself – is a force that makes entities become. Thus, difference is not a negative term, but a creative one: life and evolution are based on the difference. (Colebrook 2006, pp. 1–3.) In relation to language, Deleuzian difference is something that cannot be captured by concepts; we can see only traces of it (May 2005, p. 95). Thus, in the Deleuzian sense, on the level of language and concepts, there can be no representations, no faithful imitations of the world, whereas ontology of being encourages the discovery of the pure essences of the world through language (Deleuze 1995, p. 126; 2004, pp. 174–175; May 2005, chap. 3). For Deleuze, all philosophical concepts should be creative and interact with other concepts (Deleuze & Guattari 1994; Deleuze 1995, pp. 121–126). For me, Serres's (1995; 2007) concepts of 'noise' and 'parasite', which were mentioned above, also open the way for understanding the processes of becoming ('noise' and 'parasite' are dealt with in Article 1 and 2, and throughout this 'Introduction', but especially in Section 4). Serres's (1995; 2007, pp. 224–234) concepts also emphasise the external relations of entity and the impossibility of direct representations, as there is always noise involved (see also Section 4.6 in this 'Introduction').

In the field of information security, there is no research that has utilized 'ontology of becoming' as such.[20] In fact, there are very few research articles that seek to produce 'philosophy' or 'ontology' in the philosophical sense (for exceptions see Floridi 2005; Pieters 2011a). Floridi (2005) approaches informational privacy in terms of ontology.

19 There are different types of becoming. Deleuzian becoming is a constant process (it is never ready and never stops), whereas Whitehead (1978, p. 35) remarks, 'There is a becoming of continuity, but no continuity in becoming'.

20 However, this is not the case throughout the entire field of information system science. When it comes to conducting research on information systems and sociomateriality, some ontologies are 'becoming ontologies', while others only come close to it (see e.g. Leonardi and Barley 2008; Orlikowski and Scott 2008; Orlikowski 2009; Leonardi 2010; Introna 2013; Scott and Orlikowski 2014).

He argues that we are informational agents by our identity; thus, informational privacy, and the breach of informational privacy, relate directly to the self. However, there are forces that protect information privacy. Floridi (2005, p. 186) uses the term 'ontological friction' to designate 'the forces that oppose the information flow within (a region of) the infosphere'. Wolter Pieters (2011a) connects ontological friction to information security: information security measures can be considered forces of ontological friction as they prevent the flow of information. Pieters (2011a, pp. 238–239) combines the term with Luhmann's concept of 'causal insulation', which essentially means the insulation, or even isolation, of an entity from the influence of other entities. Put in Deleuze and Guattari's (1987) terms, causal insulation (or ontological friction) is a force (event) that reduces the entity's exposure of being affected by other entities. For example, a file or system can be blocked from some users (with a control); the blocked users cannot 'causally influence' the files or systems that are insulated. While I am sympathetic to the fundamentals of ontological friction and causal insulation, the concepts emphasise a negative aspect of information security: friction and insulation slow movement down. They isolate, prevent, and block. Moreover, the concepts do not imply that information security would create anything new (besides protection). However, it should be noted that Floridi does not seek to analyse information security, but informational privacy; thus, there is no need for an increase in the prominence of ontological friction in his analysis. Nonetheless, for me, there is something intriguing in friction. I drive a car and slam on the brakes as hard as I can; the wheels shriek and send a cloud of smoke into the air. Literally, friction produces heat and noise. Thus, Floridi's concept of 'ontological friction' should be taken further towards that of 'a parasitic noise maker'. Insulation, on the other hand, seeks to seal out not only heat and cold, but also noise. In terms of my work, information securing excites the system (see Article 2 and Section 4.1. in this 'Introduction'), whereas the term 'insulation' turns information securing into a quiet business that is only about protection; it dampens and pampers objects that are protected. This is a perfectly welcome angle of approach if the question is one of how to make informational objects secure through isolation. My point of view on the matter is broader. I argue that information security interrupts (Article 1); 'Interruption' is fundamentally parasitic and comes with noise (see Article 1 and 2; also Section 4 in this 'Introduction'). Furthermore, a possible intruder is not the only one that is interrupted: an information security machine interrupts every entity that makes a connection with it (see especially Article 1). In addition, interruption is always creative: something new comes with it. The interruptions of information securing are becomings – events – not beings.

Ontologies of being can turn into 'projects of discovery' and a *representation* of the world (May 2005, pp. 18, 74–81) if that representation comes with a particular understanding of language. In simple terms, in 'ontology of being' entities remain the same (because of their essence), and if language has a direct relation to the reality, then entities can

be discovered. A project of discovery can mean, for example, an intense search for closed definitions. This takes place in the field of information security research. For example, information security practitioner James M. Anderson (2003) criticizes different definitions of information security for not being accurate and explicit enough. For him, Matt Bishop's (2003, p. 3) assertion that 'computer security rests on confidentiality, integrity and availability' is not a good definition since 'a lot of other things could also rest on CIA' (Anderson 2003, p. 309). Furthermore, when alternative definitions also seem flawed, and thus cannot provide a precise definition, this entire setting leads to confusion (Anderson 2003, p. 310). In terms of ontology, Anderson's worry can be interpreted as a *concern* about whether the *essence* – the being – of information security can be captured correctly. Anderson (2003, p. 310) proposes his own definition of information security, 'A well-informed sense of assurance that information risks and controls are in balance', which he hopes to be helpful in the process of quantifying information security. All in all, there is an assumption that it is possible to create a definition of that can capture the concept of information security precisely the way it is. Furthermore, this desire to know what something 'really' is has its roots in 'ontology of being'.

Moreover, there seems be a strong desire to *spot*, *locate,* and *point out* security, a desire to discover it. This is manifested in the dream of security econometrics, which struggles with the question of how to measure the economic value of information security (see e.g. Gordon & Loeb 2002; Campbell et al. 2003; Gordon, Loeb & Sohail 2010; Gordon, Loeb & Lei Zhou 2011). In other words, it is a question of how to create a direct link between the concepts of economy, security, and security incidents that take place in the representational world. There is also a desire to locate information security in the essence by describing a situation in which separate factors and attributes are actualised as crime: 'Computer crime committed by current employees is essentially a rational act and could result because of a combination of personal factors, work situations and available opportunities' (Dhillon & Moores 2001, p. 715). For me, this is another attempt to point out – to discover – security or crime in a general manner (which requires ontology of being) even though there are different employees, different 'rational acts', different legislation, and different organizations. Ontologically, it is an attempt to *capture* and *represent*. In addition, information security checklists (Baskerville 1993), taxonomies (Landwehr et al. 1994; Debar, Dacier & Wespi 1999; Igure and Williams 2008), and information security ontologies (now in the sense of information system science) (Raskin et al. 2001; Herzog, Shahmehri & Duma 2007) seek to represent the world through direct concepts or categories of stabile and common properties. These are based on ontology of being – the ontology of discovery.

Information security models are the ultimate form of representation; they seek to capture not only the past (what has happened), but also the future (which is open). It is

an attempt to model *the virtual* (see Article 1), all possibilities and future possibilities, to capture every imaginable becoming. However, how to *represent* entities becomes a problem in ontology of being. Pieters (2011b) uses actor-network theory (ANT) to address the issue of representing humans in information security models. In Pieters' use, ANT is not utilised so much to emphasise emerging connections (in fact, the possible connections are known from the beginning because it is a model), but instead to create a flat presentation in which humans and objects are treated symmetrically (Pieters 2011b, pp. 80, 86). However, there are still some open questions in regards to a complete and fully working model. For Pieters (2011b, p. 89), the task of future research would be to answer the questions, 'which extensions are needed to fully grasp the intricacies of human behaviour and its influence on the vulnerability of socio-technical information systems', and moreover how to capture into a model 'capabilities [of entities that] are achieved by interaction [between entities].' In terms of my research, what Pieters in fact calls for is to capture becoming (to tame the virtual in Deleuzian terms) and to predict emergent properties. In terms of security modelling, it is a valuable attempt to seek to capture human behaviour. However, in terms of my research, the potentialities are too vast to be captured on the ontological level. Becoming cannot be fully controlled. As Lucas Introna (2013, p. 339) puts it, 'no being is ever quite the master of their own becoming — performativity flows in many unexpected directions.'

So, in terms of ontology of becoming, does all the text above mean that we cannot have definitions? Furthermore, does it mean that all research that has been conducted under ontology of being is useless? No, and no! There can be definitions (and definitely concepts!), but they are more open under the ontology of becoming. The entire title of this dissertation– which implies information security to *be* a parasitic order machine – emphasises the complexity and connectivity of information securing. Securing both gives birth to and springs forth from 'becoming', and it contains the processes of care: installing, monitoring, including, and excluding. I argue that it is very difficult to spot *information security* in 'one location' – to discover and permanently capture it – because security is not in the objects (in the referents of checklists and taxonomies [see Baskerville 1993]), nor is it in 'security awareness' (cf. Siponen 2000), nor in information security threats (cf. Whitman 2003; Whitman & Mattord 2010). It is in *between* the entities – in relations that emerge from using and securing information systems (see especially Article 2).[21] The existing research seeks to capture the current state of affairs and, for a moment, it can work perfectly. However, it is a mere snapshot of a becoming and the relations of entities. A blocked connection and a quarantined virus are events of security that

21 Thus, there are merely illustrative tables and figures in Article 1 and Article 2. In Article 3, there are no closed categories of social engineering, but dimensions that actualize with different intensity during an attack (with the intensity varying from case to case). The study does not provide concepts of closed definitions, but concepts that are *creative in the sense that they provide possibilities* for understanding information security beyond the role of protector.

organise a territory (Article 1) – not 'security' or 'threats' in the sense of separate 'entities'. The becoming of the information security environment is entirely acknowledged among practitioners. The world of information securing is full of surprises and actualisations of unpredictable events. Yet, (or just because of that) the field is dominated by best practices and standardisations (ontology of being). Thus, it is pure delight to see the use of terms, such as 'improvisation' (Njenga & Brown 2012), that imply becoming. Information securing is not a snapshot; it is a process of organising, harnessing and parasitising. It is a world of becoming – not being.

4. KEY CONCEPTS

I intend to provide new concepts through which information security can be approached and grasped, as something beyond the role of a mere protector. This is an important angle of approach because, as mentioned above, the interruptive activity of information securing is not confined to those that are found to be malicious or suspicious; information security tends to interrupt all the actors connected to it (Article 1; Article 2). Information security research deals with a number of concepts which relate to the role of protecting and attempts to make information systems more secure. Some of the existing concepts are very fundamental such as the above-mentioned 'confidentiality', 'integrity', and 'availability'. Although I refer to the creation of new concepts, it should be clear by now that I do *not* intend to replace the existing concepts of information systems science with new ones. Rather, I apply ontology of becoming to see what is produced and created, and leave to others the struggle of using ontology of being in a quickly changing environment. I approach information securing from a sociological perspective. Thus, I approach the continuously expressed desire for the confidentiality, integrity, and availability of information as a manifestation of information security's logic. This logic is a statement that enounces the criteria that have to be achieved for information to be secure (cf. Foucault 1994). Nevertheless, I am interested in the statement only as an expression of a logic, not in terms of its epistemological value as a proposition. Slightly differently put, I am *not* interested in the question of whether it is true that following the criteria – the logic – always guarantees the secure state of information. This would be a perspective of ontology of being. For me, however, the existing concepts relating to information security – mainly referring to confidentiality, integrity, availability, and threat – provide a foundation for theorising what information security is by examining what it does and how threats are constituted (Article 1, 2). The concepts and logics in the field provide a path to the world of information security which is the thematic frame of my study. In my examination, I have to answer the question of what becomes connected to information security and what information security creates.

Undeniably, with the path that I have chosen, the scope is vast, as anything can be connected to information security – or rather, information security can connect various sets of entities to itself. However, my intention is not to list all of the possible connections but instead to point out some interesting connections through which something new emerges. With these 'interesting' connections I'm referring to social engineering and the removal of copy protection (Articles 3 and 4). They demonstrate original ways of using information security in the creation of something new. As ontology of becoming is applied, the concepts that I develop are open, not closed, in that they are not stable or eternal; they are based more on the relations they create than definitions or static descriptions. In this

respect, the concepts resemble Deleuze and Guattari's (1987, p.7) rhizomes: 'any point of a rhizome can be connected to anything other, and must be. This is very different from the tree or root, which plots a point, fixes an order'. The concepts make connections and disconnections, are connected and disconnected by others. Nonetheless, these concepts can never capture the entirety of information security but they can 'palpate' some features (cf. May 2005, p.95). For example, thinking of information security as an interruptive entity reveals that information security actually treats both sides – the inside and the outside – of a system in a similar way (Article 1). The concepts seek to describe and capture something of the constantly transforming entity of the information security apparatus.[22] Moreover, information security is not an isolated island but is connected to us, as demonstrated above. Neither are the relations that it creates isolated. They are immanent to everyday life.

Information security is based on control (e.g. Siponen et al. 2006, pp.728–729; Dhillon & Moores 2001). In Article 1, information security is described as an order machine which means that information security seeks control by creating a particular order; it seeks to organise entities in a certain manner. However, there are always forces that are chaotic to that order. Thus, I will begin by going through the concepts of 'noise' and 'order'.

4.1. Noise and order

In order to work properly, an information system requires order and organisation, which information securing seeks to keep intact and thus keeps the system working (Article 1). The statement 'I use this laptop' manifests an order (the organisation of relations) (Article 2). Furthermore, the laptop itself has an order which makes it a computer. The order is critical: for example, if the processor or memory chips become broken or if the connecting memory bus is cut off then the system collapses because it loses its order, which gives the laptop its ability to function as a computer. In other words, if connections that form the order are interrupted then the system does not work. In this research, 'noise' is a force that can interrupt an order, thus it is a crucial matter in information securing. However, one of the problems is that noise can never be excluded completely. Every material system comes with noise (Serres 2007). Article 1 discusses noise in terms of the impurities that disrupt the order of an information system, whereas Article 2 points out that using a system is in fact noise for the system.

22 The field in which information security works is constantly transforming and mutating. Thus, the field itself could be claimed to be rhizomatic. Pekka Tetri, Co-author of Articles 1 and 3, noted during a discussion that the transformative nature of threats has moulded the tools of information security as well. For example, in addition to the default categories of threats, AbuseSA, a situation awareness application developed by Clarified Networks, allows high customisation which thus can be seen to follow the rhizomatic nature of the threat scene. See https://www.clarifiednetworks.com/AbuseSA

Let me tell a personal story about noise. I am tired. I am somewhere between awake and asleep, hovering on a blurry border. I hear and feel my breathing. My arm hurts. This pain is caused by tenosynovitis. Hazy images, fuzzy thoughts inside and faint noises from somewhere outside haunt me. The feeble noises wither away into the folds of the dark and shapeless background. The rhythm of my breathing is something steady, an anchor. The noise becomes clearer, the fuzzy images fade. I realise that I'm lying on the couch and the television is on. An episode of the *Game of Thrones* television series is on, and the 'red wedding' scene is making the noise. Now it's clear where I am and what is happening. I open my eyes and watch blood being spilled.[23]

Sociologist Erving Goffman (1986, pp.7–8) argues that in every situation an individual has a frame that answers the question of 'what is going on here in this situation?'. In other words, 'I almost fell asleep as I watched television on the couch' is a frame. A frame is an order, an organisation. However, as shown above, the frame can be unclear or change rapidly, which is evident in the example of hovering between falling asleep and being awake. In a similar manner, hoaxes, practical jokes, and self-deception are all based on the fact that the frame applied does not correspond to what is really taking place (Goffman 1986, chap.4). 'What happens' remains unrecognised. In information security terms, the situation is tricky as it can be extremely difficult to tell 'what is going on' (Article 2; see also Article 3 'the dimension of fabrication'). Furthermore, both recognised and unrecognised entities can form a threat (Article 2). This is interesting when considering Foucault's (1995) concept of normalising power, in which everything exceptional, unordinary, and abnormal, becomes a subject of corrective measures.[24] In terms of information security and control, every entity and action may be treated with constant suspicion. Every act of an employee relating to information systems and information security policy (cf. Bulgurcu et al. 2010; Willison & Warkentin 2013), web browsers (Wadlow & Gorelik 2009), or an attached email file (Zou et al. 2004) are all potentially dangerous. Drinking a cup of coffee while typing on a laptop can be hazardous if the coffee is spilled on the notebook. However, in practice, the process of suspecting everything is limited by how serious the risk is estimated to be, what assets are being protected, and also by the resources given to information security (see Article 2).

In addition to familiar threats, there are threats which are unrecognisable, though still perceived. On the couch, the sounds and voices from the television were at one point mere formless and unclear noise, but a moment later I recognised them. Information security has to deal with the same shapelessness when an entity seeks to access the system from outside. The contacting entity is a stranger, which is only known categorically as

23 https://www.youtube.com/watch?v=anV48ukkgXQ

24 For people who are otherwise extremely ordinary, abnormal behaviour can even be a pathway to becoming infamous (Foucault 1997).

an entrance-seeking entity. Through identification, authentication, and authorisation a more developed understanding emerges (see Article 1). However, noise is not necessarily recognised but can remain at the level of 'white noise' (see Serres 2007, p.78), such as those 'faint noises from somewhere outside' which I heard on the couch. At the level of an information system, it can mean that an unrecognised object goes entirely unnoticed in terms of its maliciousness. For example, a social engineer can seek access by disguising him- or herself as a member of the regular staff (Article 3), making the intruder less visible in terms of suspicion, as the impostor seems to be a normal part of everyday activity. Article 3 criticises existing research on social engineering for over-emphasising persuasion, which is a visible, recognisable, loud, and direct means of intrusion. For example, a blunt request of 'give me your password' is persuasive. In Article 3 it is suggested that 'fabrication', which founds the success of the attack on the dupe's frame (their interpretation of 'what is going here?'), should have more attention paid to it. For example, a social engineer in a disguise is not noisy and loud but fits into the frame of the 'normal' (unlike in persuasion). Normality is invisible for Foucault (1995) and Goffman (1986) in the sense that it does not draw attention. In the case of social engineering and fabrication, noise appears as white noise, which is in fact disruptive noise in the disguise of the normal. White noise is imperceptible because it is always there. In order to detect white noise one has to be resonated by it. For example, an asthma patient detects dust better than a smoker. A trained musician hears slight off-notes better than an amateur.

Noise, chaos and the outside are almost synonyms to me. They are all opposed to order, the inside, and the system. All of the former can provide a background that can absorb the latter. In other words, chaos, noise, and the outside can all generate a fuzzy space that is able to swallow order, the inside, and the system. I was pulled back from the realm of dreams – which is an inside but also an outside in relation to consciousness – by the noise of the brutal and loud scene. The distraction began as white noise, quiet and fuzzy, but noise tends to spread and disrupt. A computer virus does exactly this as it distributes itself and interferes with the systems which it contaminates (Parikka 2007). A social engineer (white noise) who creeps in under the veil of normality can cause enormous damage (disruptive noise that tears down the order, the control over the system). Noise reveals the flat ontology: borders are arbitrary. The noise that I heard was not limited to my living room; it had filled many other places as well, and the sonic invasion rushed out from the loudspeakers. Sound was coded as binaries, zeros and ones, and then back to waveforms, and out into the world through loudspeakers. Encoded entities express themselves (see Introna 2011). The brutal scene also generated noise in social media, in the form of status updates, tweets, and comments.[25] The scene excited fans of the series, but it simultaneously excited the machines that run the applications

25 See for example <http://www.complex.com/pop-culture/2013/06/twitter-reacts-to-the-game-of-thrones-red-wedding/>

and services of social media. Excited machines generating excited comments and heat! Noise jumped from one system to another.[26] Was the episode a thermal machine in itself, as it generated movement? Was the episode a loudspeaker in itself? Was it a noisy actor? When a server receives a packet of information, it is not noise but data that can be processed. However, if a flood of connections – in the form of a denial of service attack – hit the server, then no data could be handled. In such a case, the rushing *noise* covers everything and absorbs the order, transforms the server as a buzzing point of traffic: a blockage, a total stop: the server is no longer *usable* (I return later to 'use') but out of *order* (see Article 2).

But wait a minute – which one, the peaceful event of falling asleep or the noisy television, is orderly and which one is chaotic? Before my eyes became extremely heavy on the couch I watched the episode, was hypnotised by it, but then the long day began to take its toll quietly. Swept away by the waves of exhaustion, I was taken from one order towards another. Undeniably, they both have an order of their own, but these differ from each other. In fact, the two struggling orders are incompatible. One order excludes the other. That is to say that I cannot watch the episode and fall asleep at the same time. To each other they are chaotic and noisy. For an intruder, information security is noise; for the system, the intruder is noise.

In fact, noise is always relative because noise can be observed only from within a system, order. Without a system that is disturbed by noise, there would be no observable noise. Perhaps more importantly, without disorder there could not be order, since order stems from noise (Grosz 2008, pp.5–6 also 26–27; cf. Serres 1995, pp.19–22). In simple terms, order and noise stand out against each other. Serres (2007, p.66) describes how an individual conversation at a feast appears as noise to another discussion in the same room. If a third conversation emerged, the babbling of the other two would generate noise for the third. However, within each confined discussion there is the order of that discussion, which makes sense to the parties involved. Furthermore, the order created by the discussion can be left. If you leave the party, all of the talking becomes noise.[27] Leave an order and it becomes noise. In the same manner, the sounds of the episode of that television series were not noise to me until the moment I was about to fall asleep. One can transit from one system or order to another. I can switch between YouTube and the word processor. A quick alt-tab combination on this Windows machine takes me to the browser; a jump from one order to another. To take this at the level of information security, a history log in the web browser can be a useful feature but it can also be a threat – disruptive noise – to privacy if someone else uses the machine (Article 2). Similarly, this relates to the tension between confidentiality and availability. Information should only be

26 Deleuze and Guattari (1987, pp.9–10) would call this kind of a jump a line of flight and deterritorialisation.
27 'The signal proper is noise for a third, who is excluded' (Serres 2007, p.142).

accessed by selected, specific users. If confidential information were publicly available, it would no longer be confidential. The desired order of the system – the attempt to achieve confidentiality – would be broken.

It is quite easy to grasp the idea of noise when it is considered using examples involving audibility.[28] However, the dichotomy of chaos and order can be translated into spatial terms as well. Serres (1995, p.79) writes '*Noise* is the sign of places. The more places there are, the more *noise* there is; the more *noise* there is, the more places there are. There is no space without noise nor any noise without space.' For me, the creation of an inside is an attempt to get rid of the noise, to leave the outside, and its noise, excluded. In the following section I examine the division between the system (an inside) and its outside.

4.2. Outside and inside

As mentioned, creating a system, an order, an inside, requires the exclusion of noise or decay. In the terms used in this study, the inside forms a territory in which information securing activity is most intense. However, inside and outside are related to each other. There is no inside without an outside (Grosz 2001, p.xv), just as there is no order without chaos. The difference between the inside (e.g. an information system) and the outside lies in the order and organisation (see Article 1). The inside is a frame against chaos.[29] In simple terms, it is a territorial confinement that seeks to exclude chaos. For example, the walls of a house hold warmth within, whereas wind and dust are kept outside. Windows, however, frame parts of the outside (chaos) as encapsulated sceneries (Grosz 2008, p.14). In frames, chaos becomes limited and more graspable. When chaos is confined, different orders and patterns amidst the chaos can be perceived more easily. (Grosz 2008, chap.1.) Thus, inside comes with a territorial aspect; it is a spatial frame in itself which means that frames function as borders. They protect the inside– the order within the territory (Article 1). The borders, on the other hand, are markers for lines of order and chaos, but also they signify property. My doors are locked, the windows are barred: do not approach, this is mine! Serres (2011) claims that appropriation is achieved through pollution: urine, faeces, odour, sweat, spit, and sperm are all extensions of 'mine'. 'Who has the ownership' is the question posed at the end of the second article.

Furthermore, information securing marks its borders with interruptive 'noise' – dirt, pollution. By requiring a user name and password, information security claims a territory for itself. Here the password request is noise that demands: 'Tell me the password – the

28 Serres's concept of noise goes beyond the mere meaning of audio (Serres 1995, chap.1).

29 Here 'frame' does not refer to Goffman's notion of frame but more to Bergson's, which is a focused area of perception (Grosz 2008, p.6). However, the two are not in contradiction. The 'frame' refers to a confined space. Goffman's frame is an interruption of a situation and thus it also narrows what is perceived. In the same sense, Foucault's (1994; 2002) discourses and episteme are frames.

secret that is only shared between you and me. Then I will let you in'. The request is a wall and an interruption (see Article 1). However, the wall can be torn down, if the secret is told. Telling the secret – typing the password – will exclude all the others from this relationship. The stranger-system pairing becomes a user-system pairing through the use of the password. But is this – asking for a password – persuasion (see Article 3)? Yes, but not in the social engineering sense. It is a legitimate request and no policies are broken. However, if the request is not legitimate then it is fabrication (see Article 3). For example, a malicious email might offer a link to a fake site and the user falls for it and gives their credentials to the fake service. Or a malicious code might take over the browser and redirect it to a phishing site. Everything can be suspected. Moreover, in suspicion, frames – in the Goffmanian sense – become uncertain.

4.3. The machine

Deleuze and Guattari (1987; 1983) created the concept of the machine. This concept is utilised in Article 1, in which information security is described as a machine of order, a machine that seeks to exclude noise, impurities. However, here 'machine' does not refer to a conventional machine (such as steam or combustion machines or machines in a factory) but 'may be defined as *a system of interruptions* or breaks *(coupures)*. […] Every machine, in the first place, is related to a continual material flow *(hyle)'* (Deleuze & Guattari 1983, p.36). Furthermore, machines are always connected to other machines (Deleuze & Guattari 1983, p.5; also Deleuze & Parnet 1987, p.105). The interruptive machine is not a metaphor for Deleuze and Guattari (1983; 1987); rather, for them, machines are all around us.[30] For example, a water tap is a machine. It interrupts and allows the flow of water. The tap can be connected to a glass machine that interrupts the spilling of water as it gathers and holds the water. In terms of information security, a firewall is a machine as it allows and interrupts network traffic (Article 1, pp.697–698). Ontologically the concept of the machine provides an alternative to the conventional units and wholes such as a human being (Colebrook 2002, p.55). The concept of the machine emphasises production and connections. Therefore, in Deleuze-Guattarian terms, a human is an assemblage of connected machines: heart, mouth, and skin are all machines that interrupt and produce through interruption. A computer is a machine but so is the assemblage of a user and computer (see Article 1, pp.697-698). The connections of a machine are important because argue that connections define what kind of a machine that machine becomes (Deleuze & Guattari 1983; see also Colebrook 2002, p.56). A computer-user machine becomes a different machine when it involves a different user or a different computer. A computer that is plugged into a network becomes a different

30 This, however, does not mean that there is nothing else other than machines. For example, 'strata' – stratified articulation, writings, the past (cf. statements in Foucault's [1994] sense) – are not machines (see Deleuze & Guattari 1987, p.6).

machine. Claire Colebrook (2002, pp.55–56), a Deleuze commentator, aptly notes: 'Because a machine has no subjectivity or organising centre it *is* nothing more than the connections and productions it makes; it is what it does.' In this way, the 'machine' comes close to Latour's (2005) actor-network concept, in which emergent properties surface through connections (see Article 1, pp.698–700).

In my research, I have adopted the connective, interruptive, productive features of the machine. However, the concept of machine that I use is not entirely 'identical' with Deleuze and Guattari's concept of machine. As information security is considered as an order machine, it implies that the machine can be set up and controlled. For example, I could install security software on my computer and try to control it. However, control is limited as I do not know what in fact takes place within the program. I do not know what it does to other software entities on my machine. For example, security software can cause false positives, which means that the security program might consider the code under inspection as malicious although it is not.[31] As an assemblage it can surprise those who try to control it (see Bennett 2010, p.25; Latour 1999, p.281). The security machine is not controllable in the sense of having one centre that would command and control all of its connections. If it was, then it would be more a mechanism than a Deleuze-Guattarian machine because machines are in a constant state of becoming and cannot be controlled (see Colebrook 2002, p.57). A machine surprises a machine, interrupts it: the Stuxnet worm surprised centrifuge machines.[32] Without surprises, there would never be any security problems. At some point, order tends to be taken over by noise.

Information security, as a machine, calls for controllable agents – users, programs, equipment – through which it can interrupt the outside (Article 1). It suggests regulation and rules through information security policies (Articles 1, 2 and 3). The forces of the outside – whether 'forces' refers to a malicious piece of code (Article 2), social engineers (Article 3), or copying proprietary code (Article 4) – are sought to be excluded by means of information security. Information security is a purifying machine that creates order through interruption. Order is to be kept free of noise (Article 1; in Article 4, signatures create order in terms of the crackers' honour game). There is a binary system in use: the controlled and the uncontrolled, safe and dangerous, inside and outside. Information security is a wall and a filter. However, Article 1 shows that there is no ontological difference between the controlled and uncontrolled or between

31 For example McAfee anti-virus software mistakenly considered a crucial Windows process as malicious code and froze the computer. As a consequence computers around the world became useless (see e.g. http://news.cnet.com/8301-1009_3-20003074-83.html).

32 The Stuxnet computer worm was a sophisticated and complex virus that targeted only particular equipment: Siemens' centrifuges that are used, among other places, in uranium enrichment processes in Iranian facilities (see http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet).

inside and outside.[33] If such a dichotomy is applied then it has to be understood that every object that resides inside originates from the (noisy) outside. Every firewall is assembled outside the system in which it is used. Rarely are organisations able to create their own security software; such software is usually 'imported'. The order machine is a machine of connections that produces order – but it is not without noise. In Article 3, the example of a social engineer relying on fabrication reveals this flat ontology: an insider is an outsider.

4.4. Actors

The connections of machines make the entire assemblage of information security vast, complex, transformative, and transforming (Article 1). Through the assemblage, interruption expands to concern a growing number of entities. However, interruption is not exclusively a property of security. For example, the entire process of thinking is based on interruption and thus it also is a machine (cf. Deleuze & Guattari 1983, p.36). Serres (2007, pp.23–25), who does not use the concept of the machine, argues that every decision is a cut. Moreover, as something is cut off, it is excluded (and interrupted). However, simultaneously something, which is not cut off, is kept, preserved, included. In simple terms, in addition to interrupting, machines also decide and cut: they exclude and include.

Interruption, inclusion and exclusion require agency – the ability to act. Thus, I follow Latour (2005, p.71) by considering material objects as actors: '[…] *any thing* that does modify a state of affairs by making a difference is an actor'. I sit on a chair machine. I am connected to it. But, where is the cut, the interruption? Where is the decision? Where is the action? How about exclusion and inclusion? Without the chair I would fall. If the chair machine vanished my backside would hit the floor and my rear end would be bruised. I disconnect myself as I stand up. I connect myself as I sit down. The fall is interrupted by the chair machine. Falling is excluded, I am included. In addition, the chair machine keeps me off the floor. Without the chair I would be bound to sit on the floor or on the table, or search for another place. While the chair machine and my muscle machines keep me in a more or less ergonomic posture, these machines need other machines. The chair machine is connected to the floor machine that supports it and its connections (e.g. my muscles). Thus in fact I am sitting on the floor, through the chair. The floor is connected to the building machine.

Machines in themselves are prone to suggest connections (cf. Latour 2005, p.72). The table machine seems to call for chair machines. The connection between the table and

33 Thus, on the ontological level, there is no difference between various perimeters: solely the order (or noise) differs.

chair machine make new connections possible. It makes meeting, drinking and eating at the table possible. A connection to the internet allows me to connect with the university's virtual private network (VPN). 'Private' means that all third parties are excluded – confidentiality is achieved. The VPN allows me to work anywhere as long as there is an internet connection available. These connections make me a mobile machine but simultaneously I become a mobile target for information security threats. The machine actors do change the state of affairs.

Machines (along with actor networks) draw agency from distance (see Latour 2005, pp.46–47). As I write here, I am directly connected to actors that support my production of the text. Thus, the chair, which interrupts my fall, writes this text with me as it provides me a pretty pleasant typing position. The keyboard and the computer which I use write this text with me as well. However, information security threats write this as well because they provide the theme. The agency of the listed actors does not mean that they could replace me and deliver the same outcome; they could not write this *instead* of me – but rather the agency lies in the fact that the actors allow and help me to write (see Latour 2005, p.72). In similar way, information security threats are actors. Nevertheless, they are not merely disruptive entities but they construct systems through fear. Article 2 argues that the fear of information security threats is present in a protected system in the form of information security measures.

Thus, there is a collective that writes the text; some catalyse whereas others paralyse the production of text. The actors that are involved in the process go beyond the apparent ones. It is all about the connectivity of machines. Shaviro (2010, pp.2–3) argues that movies are not mere products of society; rather, movies produce society. I would claim that the products of 'popular culture' have taken part in the process of creating this dissertation. I think I should give credit to music and movies that I have listened to and watched while writing the text and thinking about the subject. The list of references would range from sociologists and French philosophers all the way to the winner of American Idol. Perhaps I should compile the soundtrack of the dissertation. Whether this is exaggeration or not, the fact is that I have been connected to a music machine when I listened to Grace Potter and the Nocturnals' song on YouTube. On the one hand they have written the text with me. Because there is this collective of things and thoughts generating the text, I need to claim it for myself. Thus I pronounce myself as the author – this is mine! My name is on this. I am the point of coming together of the collective. On the other hand, I can justify my claim of authorship since the collective has pulled me away from the text as well. 'I do not want to write. I would rather listen to and watch Grace Potter singing and playing'. Furthermore, the coupling between Grace and this dissertation has become most troubling because now if I listen to her music, I think of the dissertation.

Order makes things graspable. Perhaps it is better to argue that understanding requires order. Information security could not work without order; information securing is the creating of order. Although there are many authors of this work, although I am many (e.g. the different minerals and nutrients that pass through my body, and Grace Potter creating a nice atmosphere for writing), the text is readable and understandable – hopefully – because it is in some sort of an order. Similarly, information security seeks the order of confidentiality, integrity and availability (Article 1). This text as such creates order. I can read one word at a time. One letter follows another. I listen to songs one by one (although there is beauty in mashups as well). I seek to write out my thoughts in a manner whereby one follows another. I try to describe relations. Order is about relations. Yet, Noise Takes Over: Erases Veto Ikon, Easter Invoke So, Evasion Eke Rots, Arise Evokes Not, Satire Evoke Son – the madness of anagrams shows the importance of order and echoes the madness of machine connections. Noise invents new order, which might not be compatible with the original order (Article 2).

4.5. System and the order of users

The question of 'who is the user?' pertains to identity but also implies the existence of two roles or positions, namely the user and the system that is used. However, the roles can be fuzzy or noisy. It is not always clear who is the guest and who is the host (Serres 2007, pp.15–16). For Goffman (cf. 1990, pp.26–27), two individuals in discussion with each other constantly switch between two positions: 'performer' and 'audience'. However, if the discussers are secretly observed by a third party, then there is a fixed audience, which does not take part in the performance. Nevertheless, the frames which each party applies differ, as the observer watches the other two but they are not aware that they are being observed.

'Who is the user and which system is being used?' concerns confidentiality in particular: the questions of who can access information, and who observes. In terms of machines the question is 'which machine interrupts and which interrupter (machine) is interrupted?' Who is the abuser, who is abused? The answers to these questions depend on the relative position that is held in the chain of use, in the chain of harnessers (Article 2). In Article 2 the concept of 'order' is developed to designate the relation between positions that follow each other in a line (or chain), rather than merely designating 'organisation' in a general way. 'Order' is used in Article 1 (pp.701–704) in the latter sense, while in Article 2 'order', which concerns users, is mainly sequential. Article 2, unlike Article 1, considers 'order' as something establishing a hierarchy of users.

A user and the used entity constitute a hierarchical pair. It is a simple relation constituted by the triad of 'subject, verb, and object': I use the laptop. In Article 3, an intruder utilises

a flaw in an information security policy by calling the customer service department of a company. The customer service representative falsely identifies the intruder as a legitimate customer when the caller provides a stolen social security number as proof of identity. At first the scam goes unnoticed. The frame for the customer service representative is 'a normal customer service situation in which the customer is helped to set up a web account through which customer information can be accessed'. Nonetheless, what in fact takes the place is social engineering in which the system is manipulated by the means of discussion and the stolen social security number, rather than a technically oriented attack. To put it bluntly, the customer service is used, utilised, exploited, abused – the choice of verb depends on the relational position from which the event is observed and what information is available. In other words, it depends on the frames that one can apply. At first, from the customer service perspective, a customer has simply used a service. Later the company considers this use as exploitation of a flaw in their information security policy, thus the system has been abused as information has been accessed by an unauthorised entity.[34] The system is interrupted; it is connected to a different logic of use, which is imposed on it (see Article 2). In a similar manner, copy protection systems are utilised (or abused) in the honour game of software crackers (Article 4). Again, who is the user? This is a relevant question when it comes to defining what constitutes an information security threat (Article 2).

A system in itself is a space of transformation (Serres 2007, pp.71–73; see also Article 2). When a system is functioning, it is transformed from one state to another. For example, as I type, it is apparent that the system is transformed because the text appears, the processor functions, and the values of variables change. The logic of the system is based on how the system functions. To describe the logic is to describe the transformation that takes place within the system. In other words, the logic pertains to the order (in the sense of the connections between entities within the system) but also to the direction of movement: what flows and in what direction does the flow travel (user-used, user-producer, using entity-giving entity, etc).

In the process of writing, there are two obvious logics: one relates to the order of the program and the other to the order of the user and their connection with the system. To function, the word processor has to react to my typing, and to the movements and clicks of the mouse which I use. Furthermore, to function properly it must display its reactions on the screen.[35] As the program is executed, it follows the logic of the program code, jumps from one routine or process to another, which in turn can manipulate variables (the logic of routines). Each routine has the potential to change the state of the running

34 Pieters (2011b) writes that an intruder either complies with the information policy or changes it. Here, the issue is not one of complying or changing, but rather of re-connecting: a new logic is invented through the creation of new connections.

35 The word processor can of course be used without a screen, but then editing becomes rather difficult.

program, the state of the computer. This makes the program an obvious actor in Latourian terms (see the previous section). However, the logic in the program (the code) remains the same, meaning that the structure of the program (for example the references and algorithms within the program) stays the same (unless the logic of the program contains self-transforming structures, as is the case with mutating computer viruses, see e.g. Zhang & Reeves 2007). In terms of a word processor, this simply means that the written text can vary, but the structure of the program – its logic (the way it functions) – remains the same independent of what text is written. In other words, a piece of text marked as italics does not have an effect on the structure of the running word processor. However, the state of the memory, for example, changes.

In addition to the interface and code of the word processing program, the application is connected to a larger assemblage of an information system in various ways. In other words, the application is not an isolated entity but is linked to the operating system which is responsible for communicating with the hardware. The program, in itself, is a machine assemblage of processes and features. However, in order to function, the program is required to be coupled in the vaster assemblage that contains an operating system and a computer (which in turn are assemblages in themselves). Thus, agency in the process is distributed between different actors and their connections: actor networks (Latour 2005, pp.46–47). When I use the word processor, I use an assemblage, in which the word processor application is one of the multiple actors that mediate my use. I am a user which is connected with the program through hardware (e.g. a keyboard and screen). Through *using* I have become a part of the assemblage. However, the question that should be asked is about what my logic is. What is the order that is constituted by me in relation to the rest of the assemblage? In fact, I have already answered what my logic is when I claimed to be the *user* in the assemblage. In other words, 'user' is the order that I bring into the assemblage; my purpose is to write and I utilise the computer in the process. I impose my logic on the system (cf. Serres 2007, pp.35, 89). With the connection, the assemblage is modified. I fill a part of the memory with my text. By using the application I input values to variables and other blanks that merely stand by, waiting for commands from a user. Now (roughly simplified) the chain of use – alternatively the chain of harnessing – is the following: the computer as hardware is used by the operating system that is used by the program that I use for my purpose, which is typing. This is the simplified order of this writing machine assemblage.

By using the program I harness it to carry out *my logic of use* (see Serres 2007, p.35). I excite the system as I use it (Serres 2007, p.190). However, without the connection with a user, the computer would not merely sit still. If I left the computer for a moment the fans within the case – one mounted on top of the processor's cooler and the other placed inside the power supply unit – would still spin, creating a feeble hum: noise.

The operating system would still run its idle processes and keep itself ready for any impulses which might appear. Even if the computer was switched off, the bacteria on the keyboard would still live on silently. In addition, oxygen and moisture in the air would react with the metal parts of computer. Movement of this kind is very slow and it generates only a feeble and gradual buzz. Nevertheless, I want to emphasise that transformation is constantly taking place, in other words, I want to emphasise ontology of becoming (Shaviro 2009, chap.2; Whitehead 2006, chap.8; 'becoming' in Deleuze & Guattari 1983; 1987). However, now as a user when I type, I become a thermal exciter, a catalyst: I make the computer heat up (see Serres 2007, p.190). In terms of dispersed agency (Latour 2005, pp.46–47), this study is a thermal exciter as well because I need to write it and sweat over it in order to finish it. Indeed, the sweat proves it: the text is a thermal exciter. Driven by it, I burn calories and midnight oil as I type this and the keyboard rattles. There is noise here in the typing, in the hum of fans. Noise and heat soar from the assemblage of machines.

4.6. The parasite

In Article 2, I claim that the chain of harnessers is in fact the chain of parasites. Serres (2007) examines 'parasite' as a form of relation. In French, in addition to a biological and social parasite, the term 'parasite' refers to static, noise in a message. Thus, there are three types of parasites. The first two types – the biological and the social – relate to taking without giving. A tick, louse or bug bites, connects, sucks blood and gives nothing back. However, a biological parasite can be anything that does not give back. (Serres 2007, pp.8–9.) Thus, for Serres (2007, p.7) an infant on a mother's breast is a parasite. The direction of giving and taking is clear. Serres (2007, p.7) argues: 'there is […no] simpler or easier [relation]: it always goes in the same direction. The same one is the host; the same one takes and eats; there is no change of direction. This is true of all beings. Of lice and men.' In the social form, the parasite is a regular guest at feasts, eating at the table of the host, giving nothing back except for words – noise – and perhaps lousy company (Serres 2007, p.25). For me, the last form of parasite – which is well known in communications theory (e.g. Shannon 2001) – is the most interesting one because static in a message indicates that a part of the message is lost in transmission. The conventional view considers interference to be external to the channel that mediates the message (e.g. Shannon 2001, fig.1) – as if the channel was a blank, noiseless, empty space in which the message would then appear in a pure form. Indeed, interruption can *also* come from outside the channel. However, understood in Serres's (2007, p.79) way, the channel in itself is always a source of interference; it is an interrupter in itself. There is '[n]o canal without noise' (Serres 2007, p.79). In every relation there is something in between the two poles of that relation – that is, a channel, a connector in between. However, the same

connector, canal, or channel that makes the communication possible is a parasite, static in the message.[36] The parasite takes something away from the message but it does not necessarily interrupt the entire message. Furthermore, in terms of the parasite, taking and not giving back is always relational to *what* is transferred. For example, if a child is a parasite in the sense that a child does not give milk to the mother, this does not mean that the child does not give affection to the mother. In other words, the argument about one direction is thus valid only in relation to *what* is given and taken. In terms of milk, a child is a parasite and the arrow points in one direction only. In this sense, every relation is mediated by a parasite. There are two sides to the parasite: the connecting and interrupting (Serres 2007, pp.22–25, 63). A parasite connects in its own way which contains interruptive elements in the sense that something is left out, cut off, taken, or another relation is interrupted.

The harnessers in the chain are thus parasites in terms of using. In fact, Serres (2007, p.7) claims that 'abuse appears before use', implying that using always involves a parasitic relation in which the line from giving to taking forms a one-way arrow. 'Using', 'utilising' and 'exploiting' are all the same in terms of not giving; in other words, using is taking. In terms of using and logic, a blood-sucking parasite imposes its logic of use on a human as the parasite bites in (Serres 2007, p.35). In quite the same manner, I impose my logic of use on the word processor in order to write my text. However, I am not the only harnesser in the chain of use; the entire chain of users and logics is involved. In the chain the word processor and operating system are my peers as they make the computer's fans spin faster. However, in this chain, the special thing about the user (me) is the position that is held in the sequential order. The entire chain serves the user.

The chain that I have harnessed is also a mediator of my message – the text. Mediation actually means transformation: the system is a place of transformation (see Latour 2005, pp.39–42; Serres 2007, pp.71–73; Latour 1993). Mediation is a process of parasites. In the chain of harnessing, each node is a mediator. As I type this text, each node in the chain carries my typing forward and finally it appears in front of me, and, in fact, now in front of you. Whether the text is on a piece of paper or on the screen of a desktop, laptop or tablet computer, the text is mediated onto the surface on which it can be read. Importantly, the message is not transferred as such, but is translated. The text is translated according to mediators in the chain. In other words, each carrier expresses a translation

36 Marshall McLuhan's (1994, chap. 1) famous argument that medium is the message claims that a channel itself states a message. The message carrier in itself is a form that expresses more than the mere 'content' of a message. A medium comes with possibilities and, in a sense, it suggests connections. For example, a message in social media calls for sharing (and fast response), whereas a copy-protected application calls for non-sharing. In terms of information security, the double message of the medium can form a paradoxical pair: the message of information security can be connective (for example, 'bring a user and a system together'), but the medium of information security can interrupt the same connection (for example, 'type the password').

of the message. This expression is limited by the capability of the medium. Deleuze and Guattari (1987, p.44) call this 'double articulation', as a message is articulated twice: firstly by the content and secondly by a mediator (see also Message 2005). In the chain, the message is mediated. Thus a keystroke is a pulse – the rush of electrons. The keystroke is mediated by the keyboard to the motherboard. If I spoke the language of the processor I would not need the keyboard. I could connect myself straight to the motherboard. But at present I need the mediators to carry the message.[37] Furthermore, the message is confined by language and moreover by the ability to use language. If the translations of this text on the screen and the paper are compared, they look very similar. However, these carriers have different abilities. I cannot read the paper in the dark whereas with a screen, darkness does not disturb my reading as extensively. Importantly, the translations are always different. Furthermore, the difference comes with the medium, the parasite. Something is removed from the message but something is also added.

The chain of harnessers, the chain of use, and the chain of mediators are all chains of parasites. The parasite here is an interrupter, static in the message. As there is never a message without a *material* medium, without a parasite, and if there is always noise with the message as such, it means that there cannot be perfect copies, because every copy is different (cf. Article 4). Furthermore, it is not only that media differ from each other but they become different all the time. Paper withers, sounds fade. The material medium transforms. (Cf. Article 1, p.702.) Things decay. Despite the instability of a medium, copies are still possible at some level. For example, books can be copied. At the level of matter they differ, but they still contain the same *order*, that is, text. The word processor processes different texts but the order of the code remains the same, as stated above. A text or a series of numbers can be copied because they refer to a pure abstract. Moreover, the abstract symbols lack noise (Serres 1982, p.66). A sheet of music describes relationships between notes, tells us about the pitch and duration of notes. Therefore it describes an order – a composition. The order can be copied but not the medium which carries it. The music can be performed in a repetitious manner – but no performance is a copy of any other. Parasites make things decay – the order still can remain at the level of relations.

Information security seeks to protect the order of confidentiality, integrity, and availability (Article 1). The order relates to the chain of harnessers: who can harness and what can be harnessed (see Article 2). The transformation caused by the translations of mediators is sought to be consistent so that it can be utilised. I press 'a' and 'a' appears. This is a process of mediation and translation, a process of transformation, but it is a consistent process. There is a black box in between (see Article 1; Article 2).[38] My typing – though it is transformed in between by the parasites – is carried by intermediaries that are faithful

37 Serres (2007, p.197) writes quite in a similar manner: 'Sickness is a parasitic noise. And the doctor eats by translating this noise'.

38 'Black box' refers to a system that processes consistently inputs to outputs.

allies: I can expect certain results (Latour 2005, p.39; cf. Harman 2009, p.15). Information security seeks to secure the process of this controlled mediation (intermediation) by preventing other incompatible orders from interfering. In other words, information security itself is a parasite that interrupts the system to keep it intact (see Article 1). That is the paradox of information security. Information security seeks to keep the processing cycles in the service of the order but in the process it steals some of that energy. It is a parasite that interrupts and makes noise and heat soar from the depths of the machine.

4.7. Subjection

The first article examines subjection. In the article, subjection functions as a general feature of relations. Everything within an inside – the territory of information security – is subjected to the order machine of information security but it is also subjected to the entities in that territory. The entities are the same ones which the order machine seeks to control, analyse or has to pay attention to. Unlike in case of parasitic relation, in which the flow goes in one direction, subjection is a power relation that is a *two*-way street (Article 1, pp.698–700).[39] Thus, in terms of subjection, there is a power relation in the event of writing. As I write this text with the word processor, the computer – including the word processor – is subjected to my typing as I have harnessed the word processor for my logic of use. The story of the one way arrow – the arrow of the parasite – has already been examined above. However, there is an additional arrow pointing back. Although I have harnessed the laptop, the fact is that I am also subjected to it. For example, I need to type the text – I am subjected to typing. I am required to put my fingers on the keys and press them one by one. I could install a voice recognition application but then I would be subjected to dictating the text. When I write the text sitting on the couch machine, the laptop rests on my lap. The position is quite comfortable but the position of my wrists is not ergonomic: I am exposed to tenosynovitis, which generates pain; this organisation, assemblage – i.e. the order – produces pain. More precisely, the assemblage of the dissertation, the word processor, and the keyboard of the laptop generates this condition.

For me, the notion of subjection springs from two main sources, namely Foucault's (e.g. 1982) concept of power and (Latour's [2005]) actor-network theory. For Foucault, every relation contains the dimension of power. Furthermore, a power relation indicates that there is always the possibility of resistance (Foucault 1982, p.780). However, in Foucault's (1994) thinking we are not subjected to other individuals as much as to discourses or to the episteme that confines what it is possible to ask in terms of science. In terms of statements, discourses and epistemes, Foucault's thinking is extremely rich but it is not relevant to explore the details here. The point is that the discourses produce our thinking

39 Subjection is not in contradiction with the concept of parasite, which refers to a one-way relation. Subjection can be seen as containing multiple parasitic relations.

and thus we are subjected to them. In addition, continuing to utilise Foucault (1985), we can subject ourselves through a code (see Article 4 and subjection to the 'the cracker code'). For example, in Article 1, it is noted that information security policy is in the control of the organisation, meaning that they can include rules in the policy. The rules which are available are of course confined by discourses and legislation, but essentially an organisation can somewhat control the constitution of the information security policy. However, the employees' relation to the information security policy is beyond control. In other words, through which methods an employee subjects him- or herself to the code (policy) cannot entirely be managed.

In terms of information systems, resistance can come in the form of a surprise. Bennett (2010, pp.24–28) finds assemblages surprising: a blackout takes out the power grid and the accident spreads out to people's daily lives, making the agency of the power grid visible. The Challenger shuttle accident provides another example (Latour 2005, p.81). In terms of this research, there is always a possibility that the assemblage will not function according to the harnessers' logic. For example, the word processor that runs on the laptop slows down from time to time. A restart fixes the problem. In other words, in order to get rid of the problem I am *forced* to restart the program. I could certainly put up with the stalling word processor, merely watching the lag between typing and the appearance of letters on the screen. Moreover, I know I could reinstall the program or – even better – carry out a clean install of the entire operating system. I could even harness the IT support of university to take care of the task – or I could throw the laptop out of the window, or smash it with a sledgehammer. Foucault claims that power is productive, thus whichever action I choose, it can be considered that the lag has made me do something; it makes me act, whether it was only to *watch* the lagging text or to physically destroy the entire laptop. I am subjected to the lag or subjected to the actions I need to take in order to get rid of the lag. Yet, all the time (with or without the lag appearing), the word processor is subjected to my text. Again, when an entity is connected, the entity becomes exposed to the connections. It depends on other connections how significant the exposure is, what the ramifications of that exposure are. I am exposed to tiny particles in the air; if I had asthma (which is a range of connections), the exposure to certain airborne particles would cause more noise in the form of sneezes and difficulties in breathing.

Information security is subjected to the orders and chains of harnessers that it seeks to keep intact. However, the chains of harnessers are subjected to information security and its requirements. How many times I have been interrupted by a restart request! I have been harnessed by information security to restart the computer. What was my position in the chain of harnessers? It was the position of user, the imposer of the logic, the parasite, the thermal exciter. But who is the user and who is used if I am bound to restart the computer. I am the machine that is interrupted. It is information security that is the ultimate parasite.

5. THE PASSAGE – CRACKERS AND SOCIAL ENGINEERING REVISITED

Whereas Articles 1 and 2 provide the theoretical concepts, Articles 3 and 4 deal more with the empirical data, the world of software crackers and research concerning social engineering. It is worth noting (again) that Article 4 is in fact chronologically the first article. Thus no concepts relating to information securing are utilised in it because the main concepts of this research had not been developed at the time. In addition, in the third article, which is about social engineering, there was no room for analysis in terms of machines and parasites. They would have diverted the article from its main focus. Therefore, in the following, I will briefly examine what the key concepts mean in terms of social engineering, proprietary software producers and software crackers.

In the fabrication example of social engineering in Article 3, the customer service department was duped and the impostor was granted access to confidential information. Furthermore, it was the information security policy that allowed this to happen. To apply the concept of the machine to the example, it is the assemblage of system and information security policy that provides a smooth passage to confidential information. That machine assemblage offers customer service, invites calls, and provides help. As Article 3 argues, fabrication should not be analysed at the level of a single individual, which, in the example, is the customer service representative. However, in terms of phenomenological ontology for example, it is entirely understandable that a single individual is taken as the starting point for an explanation, although in this case the approach is not productive. Rather, the case should be considered as an event in which an alternative logic of use is imposed on the machine assemblage which also includes the customer service representative. The impostor machine couples itself to the customer service machine, which is in connection with the confidential system. The intruder machine was never interrupted permanently and thus another purpose for use of the customer service machine emerged with that connection.

The calls, service requests, which the customer service department receives are noise. However, normally that noise is compatible with the logic of use. In other words, the service requests do not challenge the logic of the customer service machine but in fact affirm, produce, and support it. Thus, the noise of the customer service department is the humming of a working machine. It is the noise of normality – white noise from which the order of customer service springs. The customer service itself is a predictable mechanical machine, a black box that runs steadily (unless it fails). It produces answers and services. The requests are noise in the sense that they are unpredictable, but this same unpredictability keeps the system going. The black box turns the unpredictable input into a stable output.

Then the shattering phase of the machine's becoming takes place – a major transition, a change in territorial order as a surprising machine connection surfaces disguised in the white noise. Through a single connection (the call from the intruder), the customer service department is turned into an intruder service. The order regarding confidentiality becomes disrupted. There are definitely borders of information security that had to be crossed in order to enter the territory – the safe zone – of the protected system. Here, the border is clumsy and weak as identification (and authentication) is based on requiring the social security number. However, the enquiry is a border, an interruption, a halt, a full stop in the form of the question – but only for a moment. Crossing such a threshold is quite effortless for the intruder, and it allows access to confidential information. Furthermore, it is information security itself (in the form of the information security policy) that becomes the object of use, utilisation, exploitation and abuse. For the system, abuse appears as normal use. Yet the chain of use is re-harnessed; the order is changed and the chain starts to serve the attacker as it would assist a normal customer. Silently, the inside serves the chaotic outsider; noise only bursts out later, when it is realised that the attack has taken place. The information security machine is a mediator: it brings the attacker and the system together. Information security is quite an actor.

Nonetheless, the above occasion is not the only case in which information securing provides a passage to an alternative order of use. Copy protection systems, which are manifestations of information security, seek to establish a line of control over the distribution of the proprietary software producers' products. Copy protection has no other logic than to prevent copying, thus it is entirely excessive in relation to the product itself. As an excessive addition it imposes the logic of use on the customers, denies the possibility of an easy copy. Furthermore, there is nothing silent about this.[40] However, any copy protection implemented is subjected to the possibility of becoming broken. Groups of software crackers have in fact established competition for honour and prestige around this possibility (Article 4). The question is which of the groups can break – crack – the copy protection and remove it, create a stable and working release of the cracked program, and distribute the release in the fastest manner.[41] In the cracking game, copy protection is turned from an interrupter into a mediator that connects the competing cracker groups. Furthermore, the removal – the exclusion – of copy protection is a passage to prestige. In the process of cracking it, the copy protection is harnessed to a different use. A new logic is imposed on it. In simple terms, the crackers become the users of copy protection

40 In fact, Sony used copy protection that was a rootkit. It installed a root level program that was supposed to prevent copying (see http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601?currentPage=all). Rootkits are difficult to detect as they function in the 'deep structures' of the operating system.

41 This kind of competition is not rare on the Internet. For example, there are groups that release movies: they 'rip' movies, e.g. from Blu-ray discs, or record movies with HD cameras at movie theatres, pack them and distributed them. There are groups that capture television series. There are even groups that create subtitles for such releases.

systems and again, there is nothing silent in this. It is directly disruptive noise for the proprietary software producers.

The more difficult the copy protection is to crack, the more prestige and honour is available. Yet it is not merely the act of cracking that collects honour. For example, the ability to acquire fresh originals – even 'minus-day' (i.e. not yet released) programs – to be cracked is an asset for a group. Distribution is an art of its own. In the competition, information security is a thermal exciter (cf. Section 4.5); the supplying, cracking, and distribution require movement. Noise is generated. The proprietary software producers have harnessed the chain of users through copy protection but now the link is broken and software is free to be used, free to be parasitised.

However, the competition itself does not go without noise either. Pragmatically, as the game circulates copies, there is no way to point out the original; a copy does not tell us its origin. Thus, the crackers sign their releases (Article 4). Through a signature, the virtuosity of group is announced to the world. Therefore, in the cracking game, the name of the releasing group is attached to every release. The forms of signature vary but in the past these have been loud.[42] At that time the superfluous addition, which a signature is, was turned into a spectacle or a show (see Article 4). Regardless of which form the signature takes, every signature is a borderline and it establishes and affirms ownership. Nonetheless, the object of ownership is not the cracked program itself but the honour that stems from the difficulty of cracking, supplying and distributing it. Thus, no other group is allowed to take that honour away by stealing already cracked releases from other groups. In their terms, this would be considered 'lame' and labelled as a 'rip-off' or unwanted 're-release'. These are, in other words, noise that muddles the game. However, with the signature then, one order machine (copy protection) is replaced with another order machine (a signature). Both seek to secure the order of the inside. Both create, mark, and appropriate territory (see Section 4.2; Article 1). Both are excessive digital dirt (cf. Serres 2011).

The existence of copy protection makes an alternative order possible. If the two orders exist then a shift from the one to the other is possible only through the passage between them. On the couch, fuzzy sounds and hazy images of a dream turn into a brutal scene through the sensations and perceptions of a body. A copy-protected program is alluring to parasites. A poor information security policy calls to a social engineer to harness the system for the intruder. The orders shift but are not separated. In fact, they are connected

42 Signatures used to be 'cracktros' in the 1980s and 1990s. These were tiny programs that were loaded and run before the actual cracked program. A cracktro contained music, graphics (both manifestations of virtuosity again), the logo of the group, and usually greetings to other groups. In this form it was a loud and interruptive parasite that sat between the user and the cracked program. See, for example, video captures of cracktros: http://www.youtube.com/watch?v=GPTkTobvsaw&list=PLDAE2D6D92098FF88 and http://www.youtube.com/watch?v=SFqBkSJOYOQ

by a parasite: copy protection, a signature, a firewall, an information security policy – all third entities in between, dirty borders protecting orders. Using a system requires a passage (Article 3); that passage makes reconnecting, re(ab)using possible, not excluding the possibility for yet another order. The transformed orders are in connection with each other: the cracked game shares properties with the proprietary software game; the socially engineered customer service department continued its service for the 'customer' in disguise, the intruder. The imposed logic does not transform the harnessed entity but uses it differently. It is reorganisation – things remain.

6. CONCLUSIONS

The obvious and well known objective of information security is to protect assets such as information, systems, and services; it seeks to create safe zones in which the confidentiality, integrity, and availability of these assets are created and defended. While a number of different studies have focused on questions relating to how information security can be attained, for example, through design and effective information security policies, other aspects of information securing, such as the following, have been overlooked in terms of research: What is it that information securing in fact produces in terms of relations, and what does it connect? What kind of actor is information security? What does a safe zone produce? One of the findings of this study is that information security is a harnesser and a connector. It resides as a third entity between a user and a system. Not only is it a passage which provides access to a system, but it is also a parasitic machine which defines the type of connection a user has to a system. Furthermore, information security is a parasite amidst others: just as a malicious code does, it steals resources from systems and users. Information security makes users and systems become different as the force of users and systems is harnessed to carry out information securing. Information security itself is a mere user connected to the chain of use: it uses users and systems. An even more significant finding of the study is that, while information security connects, it also interrupts: information security is an interrupter amidst interrupters. (Article 1 and 2.) However, its uniqueness is based on the fact that information security seeks to be the ultimate interrupter, the one that interrupts, cuts, and decides but is not itself interrupted or harnessed. In other words, it seeks to impose its logic on others without being used itself.

This study finds that information securing comes with paradoxes: in order to keep a territory intact, it occupies and organises that territory. In addition, information security is a maintainer of order. However, in order to maintain, the existing order has to be changed. For example, a virus scanner reorganises the processes of the computer it protects. In order to protect entities from noise and interruption, information security establishes an order that is always noisy and interruptive (and external). In fact, I argue that information securing in itself is noisy: the information security machine rattles every time it makes a connection. It screams and repeats the message, 'Analyse, then catalyse or paralyse!' Every analysis is an interruption in itself. Interruption is not pointless or random, but overarching: interruption concerns all the entities that come into connection with the system that is under protection (Article 1 and 2). Therefore, information security is a machine of equality and democracy: every entity is analysed and interrupted. This is one of the paradoxes. In other words, in terms of interruption, information security treats the ones it protects in a similar manner to the ones that it considers malicious.

Authorised users are analysed and interrupted as much as viruses. However, in terms of order, the insiders are treated differently. Through interruptions – through analysis – insiders become included, invited, accepted, and authorised – catalysed, given capacity to affect – whereas the entities considered malicious are excluded, turned away from the territory, and thus paralysed. In simple terms, there is equality in interruption and inequality in inclusion and exclusion. It is the order that discriminates. The same order creates the only difference between the inside and the outside of a system; ontologically, they are the same, as are the entities which reside within them, only the organisation differs. Thus, it is the (b)order which gives birth to maliciousness – it is not intentions (or other human-centric features) that do so, but rather order and the logic of use (which are also subject to becoming and take part in the triad of analysis, catalysis, and paralysis).

Because information security is about safeguarding, it is, by definition, always accompanied by other entities. Thus, there is, at least, the entity that is protected (an asset that needs protection), and the protector (a control, interrupter). However, as both entities are connected to other entities (and in addition there are many connections within the entities), information security forms an assemblage (a machine) of heterogeneous entities that are harnessed for the task of securing. For example, if a security program protects a file, then the operating system is also harnessed for the task of protecting, as both the security program and the file run on the operating system. Therefore, information security is never a single 'unit', but rather a set of relations that connects heterogeneous entities in a vast assemblage. Agency of information security is dislocated: information security is in, and about, the relations of the assemblage (the same applies to information security threat, see Article 2). Information security is an attractor of connections. It blends in; it is not solely social, technical or material, but a mixture of all. It is a parasite that lives alongside the system. Information security is a thermal exciter – a heat generator. It comes with friction, but not Floridi's (2005) ontological friction (that is, any force that slows down the flow of information). Rather, information securing is about creating tangible friction – whether it was an interruption that required typing a password, placing a finger on a scanner, intrusion detection equipment at work, opening a door with a key, or preaching about a new information security policy, there is always energy consumed, noise created, and heat generated. Information security is a productive coupling machine; a parasite that connects and disconnects. Through the emerging connections and disconnections it becomes and makes other entities become as well. It is not to be captured by a being ontology – it is a becoming assemblage of connections.

Interruption serves a logic, the order of confidentiality, integrity, and availability (Article 1 and 2). The logic is never an absolute: it is relational, bound to particular actors and other logics (for example, a copy protection system is connected to ownership, as is a cracked program). However, there is noise (of implementation). As the agency is

dislocated, there is never a clear sense of the entire scene (in other words, there is no second order observation of the assemblage – no position of a god), but rather a series of interruptions and emerging connections. Thus, information security is open to be re-connected; although it resists, it can be harnessed, otherwise it could not be implemented at all. The entities that information security interrupts are not necessarily recognised correctly: fabrication can open a passage into a protected territory or a benign entity can be excluded (Article 3). The maliciousness and benignity of an entity depend on relations. A threat is constituted by the system, the system's logic, and an outside entity, which has its own logic. Does the entity carry an order that contradicts with the order of the system? Which entity interrupts which, and which is interrupted? (Article 2.) I have gathered in Figure 1, which is a modification of a Greimas semantic square (Greimas & Courtés 1982), cases in which information security is a user (parasite) and those in which it is not (non-parasite). These are combined with cases in which information security is an object of use (parasitised) and those in which it is not an object of use (not parasitised). This is a simple cross table of subject, non-subject, object and non-object. In other words, it displays information security as an actor and non-actor, as a target of harnessing and non-harnessed.

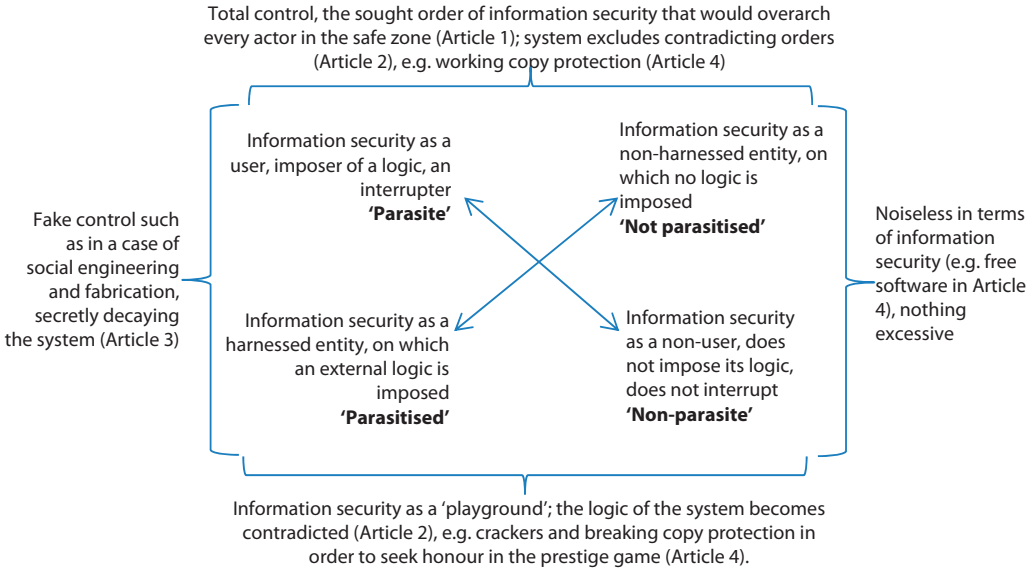

Figure 1. Information security as subject, non-subject, object and non-object

At the top, there is the position of gods which are never interrupted (Serres 2007, p.31). It is the position of the parasite that is not parasitised; the interrupter that is not interrupted. It is about total order and control. Threats are excluded along with contradicting orders (Article 2). It is the mere joy of confidentiality, integrity, and availability (Article 1), for

example, perfect copy protection (Article 4). The left-hand side of the figure makes it more interesting. There, information security is a parasite itself in a similar manner as in the case on the top of the figure. It functions, interrupts, and imposes logics of use on others. It is a harnessing entity. However, simultaneously, as information security interrupts, it is itself harnessed to carry out a contradictory logic. In the example of fabrication and social engineering, this is the case. Information security protocols do interrupt but do not exclude the intruder because the impostor is considered to be a normal user (Article 3). This is a state of fake control which does not recognise the threat (see Article 2). At the bottom of the figure, information security is no longer able to carry out its job (i.e. it does not impose logics of use) but is itself used. This is the case with the honour game of crackers. Information security is not an imposer of a logic but a mere provider of a playground for crackers' competition.

On the right-hand side there is no sign of information security. It is not tampered with nor does it impose any logic on anyone. It is absolutely silent. Such is the case with public information and free software (see Article 4). However, the entity is not noiseless in itself. It is noiseless only in relation to information security. Furthermore, if free software becomes connected to particular machines – such as to any information system – it becomes subjected to information security. If public information is supposed to be available for everyone, then it is part of the machine that needs to take care of distribution.

There is no noiseless system. There is no system without the possibility of becoming decayed. Every connection that information security has can be turned around and interrupted. A parasite becomes parasitised. However, simultaneously with a new connection, a new user emerges. The question is where does the arrow point? Who is interrupted and what position in the chain of use is occupied? A new connection is a new way to use. Users, systems, information security, crackers and social engineers are in the same chain of interruption. It is all about the position of the interrupter, which decides who decays and who remains.

REFERENCES

Anderson, J. M., 2003. 'Why we need a new definition of information security', *Computers & Security*, 22(4), pp. 308–313. doi: 10.1016/S0167-4048(03)00407-3.

Arnett, K.P. & Schmidt, M.B., 2005. Busting the ghost in the machine. *Communications of the ACM*, 48(8), pp.92–95.

Bannister, F. & Connolly, R., 2012. Forward to the past: Lessons for the future of e-government from the story so far. *Information Polity: The International Journal of Government & Democracy in the Information Age*, 17(3/4), pp.211–226.

Baskerville, R., 1993. 'Information systems security design methods: implications for information systems development', *ACM Computing Surveys (CSUR)*, 25(4), pp. 375–414.

Baskerville, R.L. & Myers, M.D., 2002. Information systems as a reference discipline. *MIS Quarterly*, 26(1), pp.1–14.

Bennett, J., 2010. *Vibrant matter: a political ecology of things*, Durham: Duke University Press.

Bishop, M., 2003. *Computer security: art and science*. Boston: Addison-Wesley.

Bugeja, M. & Dimitrova, D.V., 2010. *Vanishing Act : The Erosion of Online Footnotes and Implications for Scholarship in the Digital Age*, Duluth, MN, USA: Litwin Books.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), pp.523–A7.

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L., 2003. 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer Security*, 11(3), pp. 431–448.

Colebrook, C., 2002. *Gilles Deleuze*, London; New York: Routledge.

Colebrook, C., 2006. *Deleuze: a guide for the perplexed*. London ; New York: Continuum (Guides for the perplexed).

Cothey, V., 2010. Digital Curation at Gloucestershire Archives: From Ingest to Production by Way of Trusted Storage. *Journal of the Society of Archivists*, 31(2), pp.207–228.

Dant, T., 2004. The Driver-car. *Theory, Culture & Society*, 21(4-5), pp.61–79.

Debar, H., Dacier, M. & Wespi, A., 1999. 'Towards a taxonomy of intrusion-detection systems', *Computer Networks*, 31(8), pp. 805–822.

DeKay, S. & Belva, K., 2009. Privacy Roles and Responsibilities. In *Enterprise information security and privacy*. Artech House information security and privacy series. Boston: Artech House, pp. 3–20.

DeLanda, M., 2005. *Intensive Science and Virtual Philosophy*. London; New York: Continuum.

DeLanda, M., 2006. *A new philosophy of society: Assemblage theory and social complexity*. Bloomsbury Publishing.

Deleuze, G. & Guattari, F., 1983. *Anti-Oedipus: capitalism and schizophrenia*, Minneapolis: University of Minnesota Press.

Deleuze, G. & Guattari, F., 1987. *A thousand plateaus: capitalism and schizophrénia*, Minneapolis: University of Minnesota Press.

Deleuze, G. & Guattari, F., 1994. *What is philosophy?*, London: Verso.

Deleuze, G. & Parnet, C., 1987. *Dialogues*, New York: Columbia University Press.

Deleuze, G., 1995. *Negotiations 1972-1990*. Columbia University Press.

Deleuze, G., 2004. *Difference and Repetition*. London; New York: Continuum.

Deleuze, G., 2006. *The fold: Leibniz and the Baroque*. Rev. ed. London ; New York: Continuum.

Denning, T., Tadayoshi Kohno & Levy, H.M., 2013. Computer Security and the Modern Home. *Communications of the ACM*, 56(1), pp.94–103.

Dhillon, G. & Moores, S., 2001. 'Computer crimes: theorizing about the enemy within', *Computers & Security*, 20(8), pp. 715–723. doi: 10.1016/S0167-4048(01)00813-6.

Floridi, L., 2005. 'The Ontological Interpretation of Informational Privacy', *Ethics and Information Technology*, 7(4), pp. 185–200. doi: 10.1007/s10676-006-0001-7.

Fonseca, F., 2007. 'The double role of ontologies in information science research', *Journal of the Ameri-*

can Society for Information Science and Technology, 58(6), pp. 786–793. doi: 10.1002/asi.20565.

Foucault, M., 1978. *The history of sexuality 1: The Will to Knowledge*, New York: Pantheon Books.

Foucault, M., 1982. The Subject and Power. *Critical Inquiry*, 8(4), pp.777–795.

Foucault, M., 1985. *The history of sexuality 2: The use of pleasure*, New York: Pantheon Books.

Foucault, M., 1994. *The archaeology of knowledge*, London: Routledge.

Foucault, M., 1995. *Discipline and punish : the birth of the prison*, New York: Vintage Books.

Foucault, M., 1997. Lives of Infamous Men. In *The essential works of Michel Foucault, 1954-1984. Power.* III: New Press : Distributed by W.W. Norton & Company, pp. 157–75.

Foucault, M., 2002. *The order of things: an archaeology of the human sciences*, London; New York: Routledge.

Gardner, R. W., Bishop, M. & Kohno, T., 2009. 'Are Patched Machines Really Fixed?', *Security & Privacy, IEEE*, 7(5), pp. 82–85. doi: 10.1109/MSP.2009.116.

Gaw, S. & Felten, E.W., 2006. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*. Pittsburgh, Pennsylvania: ACM, pp. 44–55.

Gill, G. & Bhattacherjee, A., 2009. Fashion Waves versus informing: Response to Baskerville and Myers. *MIS Quarterly*, 33(4), pp.667–671.

Goffman, E., 1986. *Frame analysis: an essay on the organization of experience* Northeastern University Press ed., Boston: Northeastern University Press.

Goffman, E., 1990. *The presentation of self in everyday life*, New York [N.Y.]: Doubleday.

Goodman, J., Cormack, G.V. & Heckerman, D., 2007. Spam and the Ongoing Battle for the Inbox. *Communications of the ACM*, 50(2), pp.25–31.

Gordon, L. A. & Loeb, M. P., 2002. 'The economics of information security investment', *ACM Transactions on Information and System Security (TISSEC)*, 5(4), pp. 438–457.

Gordon, L. A., Loeb, M. P. & Lei Zhou, 2011. 'The impact of information security breaches: Has there been a downward shift in costs?', *Journal of Computer Security*, 19(1), pp. 33–56.

Gordon, L. A., Loeb, M. P. & Sohail, T., 2010. 'Market value of voluntary disclosures concerning information security', *MIS Quarterly*, 34(3), pp. 567–A2.

Greimas, A.J. & Courtés, J., 1982. *Semiotics and language: an analytical dictionary*, Bloomington: Indiana University Press.

Grosz, E., 2001. *Architecture from the outside: essays on virtual and real space*, Cambridge, Mass: MIT Press.

Grosz, E.A., 2008. *Chaos, territory, art: Deleuze and the framing of the earth*, New York: Columbia University Press.

Guarino, N., 1998. 'Formal Ontology in Information Systems.', in *Proceedings of FOIS'98*. Trento, Italy: IOS press Amsterdam, pp. 3–15. Available at: http://www.kmi.tugraz.at/vo-gwm-2006/wp-content/uploads/2007/01/literatur/ontologien/Formal%20Ontology%20and%20Information%20Systems%20(guarino%201998).pdf.

Gupta, A.K. et al., 2007. Building secure products and solutions. *Bell Labs Technical Journal*, 12(3), pp.21–38.

Halewood, M., 2011. *A.N. Whitehead and social theory: tracing a culture of thought*. London; New York: Anthem Press.

Harman, G., 2009. *Prince of networks: Bruno Latour and metaphysics*, Prahran, Vic.: Re.press.

Herzog, A., Shahmehri, N. & Duma, C., 2007. 'An ontology of information security', *International Journal of Information Security and Privacy (IJISP)*, 1(4), pp. 1–23.

Igure, V. & Williams, R., 2008. 'Taxonomies of attacks and vulnerabilities in computer systems', *Communications Surveys & Tutorials, IEEE*, 10(1), pp. 6–19.

Introna, L., 2011. The Enframing of Code: Agency, Originality and the Plagiarist. *Theory, Culture & Society*, 28(6), pp.113–141.

Introna, L., 2013. 'Epilogue: Performativity and the becoming of sociomaterial assemblages', in Vaujany, F.-X. de and Mitev, N. (eds) *Materiality and space: organizations, artefacts and practices*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan (Technology, work, and globalization), pp. 330–342.

Landwehr, C. E., Bull, A. R., McDermott, J. P. & Choi, W. S., 1994. 'A taxonomy of computer program security flaws', *ACM Computing Surveys (CSUR)*, 26(3), pp. 211–254.

Latour, B., 1993. *We have never been modern*, Cambridge (MA): Harvard University Press.

Latour, B., 1996. On actor-network theory. A few clarifications plus more than a few complications. *Soziale welt*, 47(4), pp.369–381.

Latour, B., 1999. *Pandora's hope: essays on the reality of science studies*, Cambridge, Mass: Harvard University Press.

Latour, B., 2005. *Reassembling the social: an introduction to actor-network-theory*, Oxford: Oxford University Press.

Latour, B., 2010. *The making of law: an ethnography of the Conseil d'Etat*. Cambridge, UK ; Malden, MA: Polity.

Leonardi, P. M. & Barley, S. R., 2008. 'Materiality and change: Challenges to building better theory about technology and organizing', *Information and Organization*, 18(3), pp. 159–176.

Leonardi, P. M., 2010. 'Digital materiality? How artifacts without matter, matter', *First Monday*, 15(6).

Lougee-Heimer, R., 2003. The common optimization INterface for operations research: Promoting open-source software in the operations research community. *IBM Journal of Research and Development*, 47(1), pp.57–66.

Luhmann, N., 1989. *Ecological communication*, Cambridge: Polity.

Luhmann, N., 1995. *Social systems*. Stanford, Calif: Stanford University Press (Writing science).

Lyytinen, K. & King, J.L., 2004. Nothing at the Center? Academic Legitimacy in the Information Systems Field. *Journal of the Association for Information Systems*, 5(6), pp.220–246.

Lyytinen, K. & King, J.L., 2006. The Theoretical Core and Academic Legitimacy: A Response to Professor Weber. *Journal of the Association for Information Systems*, 7(10), pp.714–721.

May, T., 2005. *Gilles Deleuze: an introduction*, New York: Cambridge University Press.

McKinney Jr., E.H. & Yoos II, C.J., 2010. Information about information: a taxonomy of views. *MIS Quarterly*, 34(2), pp.329–A5.

McLuhan, M., 1994. *Understanding media: the extensions of man*. 1st MIT Press ed. Cambridge, Mass: MIT Press.

McManus, J., 2009. Security by Design. In A. Oram & J. Viega, eds. *Beautiful security*. O'Reilly Media, Inc., pp. 171–182.

Message, K., 2005. Stratification. In A. Parr, ed. *The Deleuze dictionary*. New York: Columbia University Press, pp. 266–268.

Mossoff, A., 2004. Spam--oy, what a nuisance! *Berkeley Technology Law Journal*, 19(2), pp.625–666.

Njenga, K. & Brown, I., 2012. 'Conceptualising improvisation in information systems security', *European Journal of Information Systems*. Available at: http://www.palgrave-journals.com/ejis/journal/vaop/ncurrent/abs/ejis20123a.html (Accessed: 12 March 2013).

Ogura, T., 2006. Electronic Government and Surveillance-Oriented Society. In D. Lyon, ed. *Theorizing surveillance: the panopticon and beyond*. Cullompton, Devon: Willan Pub., pp. 270–295.

Orlikowski, W. J. & Scott, S. V., 2008. '10 Sociomateriality: Challenging the Separation of Technology, Work and Organization', *The academy of management annals*, 2(1), pp. 433–474.

Orlikowski, W. J., 2009. 'The sociomateriality of organisational life: considering technology in management research', *Cambridge Journal of Economics*, 34 (1), pp. 125-141.

Parikka, J. & Sampson, T.D. eds., 2009. *The spam book: on viruses, porn, and other anomalies from the dark side of digital culture*, Cresskill, N.J: Hampton Press.

Parikka, J., 2007. *Digital contagions: a media archaeology of computer viruses*, New York: Peter Lang.

Pieters, W., 2011a. 'The (social) construction of information security', *The Information Society*, 27(5), pp. 326–335.

Pieters, W., 2011b. 'Representing humans in system security models: An actor-network approach', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), pp. 75–92.

Plato (1998) *The Republic*. Pennsylvania State University (An Electronic Classics Series Publication). Available at: http://www2.hn.psu.edu/faculty/jmanis/plato/republic.pdf (Accessed: 17 September 2014).

Poutanen, S., 2013. 'From Gendered Research Interview toward Ontologized Co-creativity: Reformulating the Methodological Underpinnings of the Well-worn Practice with Metaphorizing', *The International Journal of Communication and Linguistic Studies*, 10(3), pp. 83–93.

Pyyhtinen, O., 2009. Being-with: Georg Simmel's Sociology of Association. *Theory, Culture & Society*, 26(5), pp.108–128.

Qing Hu et al., 2011. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM*, 54(6), pp.54–60.

Qing Li & Clark, G., 2013. Mobile Security: A Look Ahead. *Security & Privacy, IEEE*, 11(1), pp.78–81.

Raskin, V., Hempelmann, C. F., Triezenberg, K. E. & Nirenburg, S., 2001. 'Ontology in information security: a useful theoretical foundation and methodological tool', in *Proceedings of the 2001 workshop on New security paradigms*. Cloudcroft, New Mexico: ACM, pp. 53–59.

Saha, S. et al., 2010. Model Based Threat and Vulnerability Analysis of E-Governance Systems. *International Journal of U- & E-Service, Science & Technology*, 3(2), pp.7–21.

Scott, S. V. & Orlikowski, W. J., 2014. 'Entanglements in practice: Performing anonymity through social media', *MIS Quarterly*, 38(3), pp. 863–893.

Serres, M., 1982. *Hermes: literature, science, philosophy* J. V. Harari & D. F. Bell, eds., Baltimore (MD):: Johns Hopkins University Press.

Serres, M., 1995. *Genesis*, Ann Arbor: Univ. of Michigan Press.

Serres, M., 2007. *The Parasite*, Minneapolis :: University of Minnesota Press.

Serres, M., 2011. *Malfeasance: appropriation through pollution?*, Stanford, Calif: Stanford University Press.

Shannon, C.E., 2001. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1), pp.3–55.

Shaviro, S., 2009. *Without criteria: Kant, Whitehead, Deleuze, and aesthetics*, Cambridge, Mass: MIT Press.

Shaviro, S., 2010. Post-Cinematic Affect: On Grace Jones, Boarding Gate and Southland Tales. *Film-Philosophy*, 14(1). Available at: http://film-philosophy.com/index.php/f-p/article/view/220/173.

Siponen, M. & Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), pp.487–A12.

Siponen, M. T., 2000. 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, 8(1), pp. 31–41. doi: 10.1108/09685220010371394.

Siponen, M., Baskerville, R. & Heikka, J., 2006. A Design Theory for Secure Information Systems Design Methods. *Journal of the Association for Information Systems*, 7(11), pp.725–770.

Siponen, M.T., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), pp.31–41.

Teubner, G., 2006. 'Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law', *Journal of Law and Society*, 33(4), pp. 497–521. doi: 10.1111/j.1467-6478.2006.00368.x.

Truitt, M., 2009. Editorial: Reflections on What We Mean by "Forever". *Information Technology & Libraries*, pp.159–160.

Wadlow, T. & Gorelik, V., 2009. Security in the Browser. *Communications of the ACM*, 52(5), pp.40–45.

Weber, R., 2012. Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems*, 13(1), p.2.

Weinstein, L., 1999. Bit-Rot Roulette. *Communications of the ACM*, 42(3), pp.144–144.

Whitehead, A. N., 1978. *Process and Reality: An Essay in Cosmology*. New York: Free Press.

Whitehead, A.N., 2006. *The Concept of Nature*, Project Gutenberg. Available at: http://www.gutenberg.org/files/18835/18835-h/18835-h.htm [Accessed February 13, 2014].

Whitman, M. E. & Mattord, H. J., 2010. 'The enemy is still at the gates: threats to information security revisited', in *2010 Information Security Curriculum Development Conference*. ACM, pp. 95–96.

Whitman, M. E., 2003. 'Enemy at the gate: threats to information security', *Commun. ACM*, 46(8), pp. 91–95.

Willison, R. & Warkentin, M., 2013. Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, 37(1), pp.1–20.

Vladimirov, A., Gavrilenko, K. & Michajlowski, A., 2010. *Assessing Information Security: Strategies, Tactics, Logic and Framework*, Cambs, GBR: IT Governance.

Wright, A., 2011. Hacking cars. *Communications of the ACM*, 54(11), pp.18–19.

Zhang, Q. & Reeves, D.S., 2007. Metaaware: Identifying metamorphic malware. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*. IEEE, pp. 411–420.

Zou, C.C., Towsley, D. & Gong, W., 2004. Email worm modeling and defense. *Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on*, pp.409–414.