Journal of the Association for Information Systems

Volume 13 | Issue 9 Article 1

9-27-2012

The Order Machine – The Ontology of Information Security

Jukka Vuorinen
University of Turku, juanvu@utu.fi

Pekka Tetri
University of Oulu, pekka.tetri@gmail.com

Recommended Citation
Vuorinen, Jukka and Tetri, Pekka (2012) "The Order Machine – The Ontology of Information Security," *Journal of the Association for Information Systems*, 13(9), .
DOI: 10.17705/1jais.00306
Available at: https://aisel.aisnet.org/jais/vol13/iss9/1

Journal of the Association for Information Systems
JAIS

Research Perspective

The Order Machine – The Ontology of Information Security

Jukka Vuorinen
University of Turku
juanvu@utu.fi

Pekka Tetri
University of Oulu
pekka.tetri@oulu.fi

Abstract

Traditionally, information security has been approached in terms of how to achieve the confidentiality, integrity, and availability of information. In this paper, we seek to ontologically examine information security by using Gilles Deleuze and Félix Guattari's philosophical concepts of machine, coupling, interruption, and territory. Through these concepts, we conceptualize information security as an order-seeking, connection-based, territorial security machine that attempts to subject and harness other actors – from technical devices and physical barriers to employees and various combinations of these actors – to carry out the security machine's protective tasks. The goal of the security machine is to block or interrupt the chaotic forces of the outside and, thus, to maintain the fragile order of information. However, the process of interrupting the outside requires interruption of the inside as well: users and organizations are interrupted daily by the security machine and its practices. Yet this aspect of information security has remained largely unexamined. We argue that the question of what information security does to its subjects – what its effects are – in the protected system should be examined more thoroughly.

Keywords: *Information Security, Spatiality, Territory, Information Security Threat, Socio-Technical Security.*

* Carol Saunders was the accepting senior editor. This article was submitted on 23rd November 2009 and went through three revisions.

Volume 13, Issue 9, pp. 695-713, September 2012

1. Introduction

In this paper, we develop a philosophy of information security, a manner of approach that discusses the ontology of information security. More specifically, we delineate the ontology of information security to provide a point of view from which new research subjects can be suggested. Most of the existing research literature on information security is driven by practical aspirations. Scholars have focused on questions of improvement; for example, on how to develop information systems so that they are more secure, or on how to prevent the abuse of the systems (Baskerville, 1993; Dhillon & Backhouse, 2001). In these undertakings, the concepts of confidentiality, integrity, and availability (CIA) have played a major role because scholars have viewed these as the chief objectives of information security (e.g., Dhillon, 2007; Stanton & Stam, 2006). Nonetheless, despite those studies that focus on CIA as the objective of information security and on how they are achieved in practice, information security in and of itself – the question of what it is ontologically – has remained largely unexamined (cf. Pieters, 2011). In this paper, we examine the ontology of information security to depict what information security is and what it does or, rather, to depict what it is through what it does. That is to say, we commence from the idea that information security is not a neutral entity; that is, it is not additional to or parallel with information systems but is in itself active and productive.

Information security has become a part of everyday life. Organizations use significant quantities of resources to build up a sturdy information security system. Users in organizations and at home invest time in carrying out practices related to information security; for example, entering passwords and pin codes, updating software with the latest security patches, and dealing with suspected phishing emails. Moreover, as new technology is introduced, new security issues arise (e.g., viruses, mobile phone theft). Thus, information security is a transformative and pervasive entity.

Due to the ways in which information security territorializes different spaces (from homes to large organizations), interrupts threats (e.g., to keep information available only to authorized users), and connects users (e.g., a user connecting to an email account through information security), we believe that utilizing Deleuze and Guattari's concept of the machine and territory in order to grasp some ontological features of information security is productive. The ontological approach – that is, the description of information security's material and conceptual functions – questions whether information security is a mere protector of information. In other words, we argue that information security goes beyond its role of providing CIA because through its activity it increases the complexity of the system in which it is implemented. An ontological analysis reveals these additional roles. For example, information security can be problematic when it comes between a user and information, when it requires constant updating, or when those who use it require constant education. Moreover, by employing the concept of the machine and analyzing territorial, spatiotemporal features of information security, we develop new concepts and connections that reveal different aspects of information security and provide help with the future analysis of information security as a productive actor. This conceptualization provides a possibility for a new research problematization in which information security in itself is seen as a problematic actor as it comes between a user and a system. Through this problematization and through the future research that can be generated by it, we can improve our understanding of information security.

In Section 2, we introduce the concept of the machine, and explore machines in information security and how everything that becomes connected to information security also becomes subjected to it. Moreover, we claim that individuals become modified by this subjection. In Section 3, we analyze the territorial nature of information security in spatial and temporal terms. Information security never exists in a void but always requires a material medium (data territory) and agents to achieve the order that it seeks. The agents, who organize safe zones in which data territories are situated, also exist in space and time. In Section 4, we also look at how another spatial category, the perimeters between the inside and the outside, connect or entangle with each other in information security. Finally, we discuss the implications of this; that is, potentially fertile research subjects based on our suggestions.

2. Some Features of the Machine

The French philosophers Gilles Deleuze and Félix Guattari (2004a) created the concept of a "machine". For us, it provides a conceptual tool to approach security and information security in a novel manner; that is, to examine information security itself as a productive entity. Applying the machine concept to information security opens up a viewpoint that describes, in its own manner, the security landscape and helps us to understand security activity as a whole. Although we use the notion of the machine as a methodological tool, the security machine exists materially and has concrete ramifications. The first task is to outline what the machine is.

Deleuze and Guattari (2004a, pp. 2, 5–6, 38–39) claim that a machine has a function, which is to produce and interrupt (cf. Serres, 2007, p.11). They use the example of a mouth as a machine (Deleuze & Guattari, 2004a, p. 39). It can produce, for example, a flow of chewed food for the stomach. In the same way, a door is a machine in terms of physical security (which is also part of information security (e.g., Basik, 2008, pp. 60–63; Rogers, 2006, pp.13–14)). It forms a barrier between inside and outside. In the network environment, a firewall carries out the same function in a technical manner. Bruno Latour (1992, pp. 154–155) has noted that a door carries out an enormous task because it produces a temporary hole in the wall; without the door, there would only be a wall, through which it is much more difficult to enter or exit. A firewall keeps certain connections out and allows particular traffic in. In the case of a door, the stream of individuals arriving and departing flows through the temporary hole – the door. It is a machine that allows the free flow, a flow that can also be interrupted by the same machine when the door closes. In a similar manner, the flow of data packets is interrupted by the firewall. As demonstrated here, a machine can be anything that merely interrupts the flow of something – chewed food, a crowd, or information.

These Deleuze-Guattarian machines do not stand isolated but become connected to form huge assemblages[1]. Deleuze and Guattari (2004a, p. 5) actually state that a machine is always coupled to another machine. To continue the mouth example, it can be argued that the mouth is connected to the stomach (which is another machine as such); without the mouth machine, the stomach machine would have nothing to process (cf. Deleuze & Guattari, 2004a, p. 39). Referring again to information security, a door or a firewall is not an isolated machine carrying out its job. A corridor connected to the door or routers connected to the firewall are other machines that create lines of movement, allowing a spatially confined stream of people or data packets to be transferred. The limited space between the walls prevents (interrupts) the chaotic dispersion of the stream. The task carried out by a corridor becomes evident if we consider a concourse: a large hall allows a crowd to spread out.

In addition to a corridor machine (spreading interrupter, straight-line-producer), a door may be connected to other types of machines. In fact, the door (like any machine) can have multiple connection points; it may be connected to an electronic lock and logger that in turn forms a connection to an information system running in a server. The server might host several different services, such as an access control system, but it might also carry out other services as well. So a door is connected, in a direct way, to a network of other machines that form part of a security machine at a single level in space. A door with a lock denies and allows entrance, divides and creates territories (with the help of walls, fences, surveillance and other agents), while at the same time provides information about those who pass via loggers (connected to information systems). Thus, a door as such is connected to other machines, the types of which depend on what it produces. Through the connections (or couplings) of machines emerge new machines: the assemblage of the door with the electronic lock and logger can be seen as a new machine unit.

[1] In this sense, machine thinking resembles actor network theory (cf. Latour, 1996; 2005).

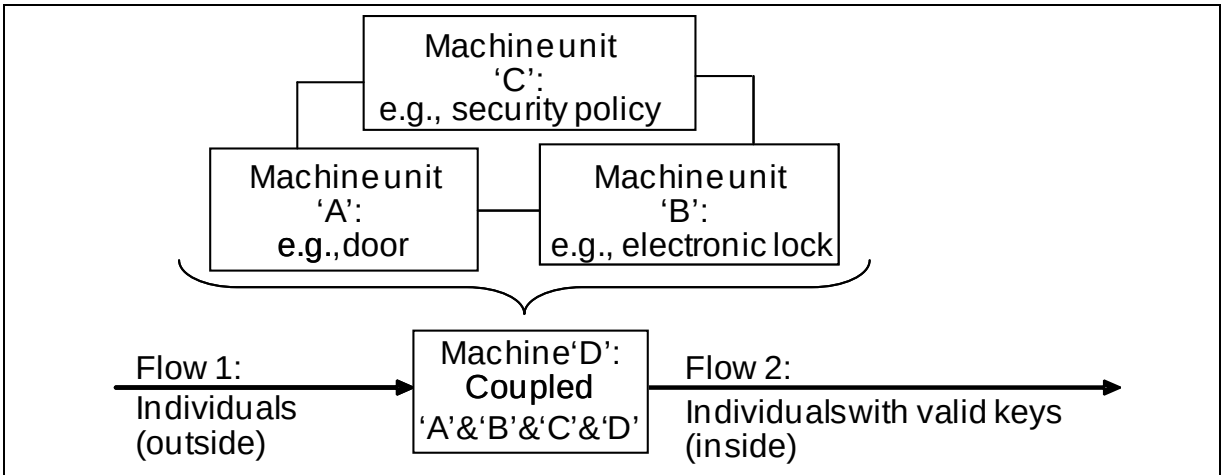

Figure 1. An Example of a Machine and its Connections

Figure 1 summarizes and simplifies the basic thought behind our concept of machine. First, there is the "Flow 1" of individuals coming in. "Machine D", which is the assemblage of separate units (door, electronic lock and policy regulating the use of all of these), interrupts "Flow 1" and produces "Flow 2". Machine D interrupts everyone including individuals with keys. By using the valid key they can proceed, while the keyless remain outside.

The couplings are connections of linked machines. Flow 1 is not coupled to Machine D but merely becomes connected to it through the interruption process of Machine D. If we use the term coupling in such a case, we refer to a connection between machines. A coupling is a connection, but not all connections are necessarily couplings because individuals or machines may become temporarily connected with other machines without being coupled. An example of this would be an individual walking through a door/lock machine: They are temporarily connected (processed by) the door/lock machine, but not coupled with it.

2.1. Connections: Emergence of Novelty and Subjection

On the one hand, one of the goals of thinking through the machine concept is the attempt to reveal what takes place in information security activity, which enables us to evaluate security processes both in their individual forms and as a whole in a combination of elements. This description of information security, on the other hand, will eventually lead us to a position from which we can problematize information security in a new manner. In Figure 1, Machine D is a new machine, a coupling of Machine unit A, Machine unit B, and Machine unit C. Machine unit C differs from Machine unit A and Machine unit B because information security policies are non-material. Thus, Machine unit C is not an exclusive property of Machine D but can be implemented in other door/lock machines as well. But Machine unit A and Machine unit B are material machines and cannot be implemented in other parallel machines simultaneously. In other words, the same door cannot exist in two places at the same time. It is, however, a part of Machine D. But if we move to a larger scale we could see Machine D, and thus Machine unit A and Machine unit B, as part of a building machine. This is to say that as machines are coupled they form assemblages and new machines: the door machine as a temporary hole, a door/lock machine as a key-controlled temporary hole, a door/lock/policy coupling as a regulated passage-control machine.

The fact that machines couple in line with other machines and that machines couple to create new machines implies that we could examine machines by dissecting them and finding new machines. An electronic lock is a machine, yet it is an assemblage of other machines. Transistors, electronic circuits, and a case in which these are embedded are all machines. The firewall is not a single machine but comprises different components. One machine is never just one machine but always multiple machines, which means that it is filled with inner connections or connected to other

machines (see Deleuze & Guattari, 2004a, pp. 45–46; cf. Deleuze & Guattari, 2004b, p. 38; Latour, 1999, p. 182)[2]. Thinking in terms of machines opens quite a chaotic view: connection upon connection, almost an infinite number of machines connected to one another. This raises the question of limits. Limits are formed in terms of the direction, density, and intensity of connections. For example, a virus scanner couples to the operating system and computer it runs on. Yet, it is separated. In the file system, it has its own files and directories or folders. The processes of the program refer mostly to its own processes: where to jump to, what to load, what routine to run. In this sense, the program is turned more in on itself than outwards and, thus, it forms an intensive whole, an entity, a dense network of connections encompassing a continuously interacting inside (cf. Pyyhtinen, 2010, pp. 43–44). This is to say that the set of small machines – pieces of executed program code – form an assemblage that appears as a one, as a whole, as a unit. Units can be considered as extractables (Delanda, 2009, pp. 10–11). A virus scanner, or a door, can be replaced with another unit. We could also change the electronic lock embedded in the door, or we could replace an electronic circuit or a transistor in the electronic lock. In summary, machines can be units in themselves and they are never isolated, but connected.

Novelty in Machine D springs from connections. Machine unit A, Machine unit B, and Machine unit C do not work separately in Machine D but are brought together in Machine D through the couplings. Placing two elements in a position of working together differs from a situation in which they are individual, unconnected elements. When they are connected, both components add something to the assemblage and to each other (cf. Deleuze & Guattari, 2004a, 2004b; Latour, 1999, pp. 179, 182–183; May, 2006, pp. 123–124, 137–139). Bennett (2010, p. 22) puts it aptly: to enter an assemblage is to simultaneously modify it and to become modified by it. The door is not the same without the lock and vice versa. Novelty emerges in couplings. Furthermore, this emergence is actualized in every event of connection and disconnection of machines, and this serves as a foundation for machine dynamics: as a machine is coupled it becomes different.

In addition to the novelty that emerges with any connection, the connections have another feature: subjection. Subjection is a line of relation and effect that exists in any connection[3]. In other words, both ends of the connection provide an environment for each other. The door is subjected to the lock as it forces the door to stay closed, but at the same time the lock is embedded and thus subjected to its environment, which is the door. If the door is wide open, the lock cannot function: the door has to be in the correct position to be locked. Subjection does not stop here because there are more connections. The example of a virus scanner and a computer may further assist readers to grasp the idea of subjection. The scanner produces an immunology system (by interrupting viruses) for the computer (see Parikka, 2007), while the computer serves as an environment for the scanner to be deployed in, to work with. As the scanner is installed on a computer, alongside the emergence of novelty – that is, the computer is not the same without the virus scanner – the line of subjection surfaces. The computer is subjected to the virus scanner since the scanner has access to the files on the computer. It may interrupt the action of the computer in the event that it detects malware. However, the virus scanner is subjected to the computer and the files on it. It has to scan the files that are transferred to the computer (see Figure 2). It is as if there was a rope tying both sides: if one moves, so does the other. The connection between the two is a positive power relation – both affect each other's activity (see Foucault, 1998, pp. 138–139). Thus, connection, emergence of novelty, and subjection go hand-in-hand.

[2] Bruno Latour (1999, p. 183) would call the process of treating an assemblage as one, with a clear input and output, blackboxing. As with everything in Latour's approach, black boxes are actants, which are defined by their effect on other actants.

[3] Our concept of subjection springs from Michel Foucault's (1991; 1998, pp. 92–96; 2002, pp. 337–342) idea of power that is a specific type of relation.

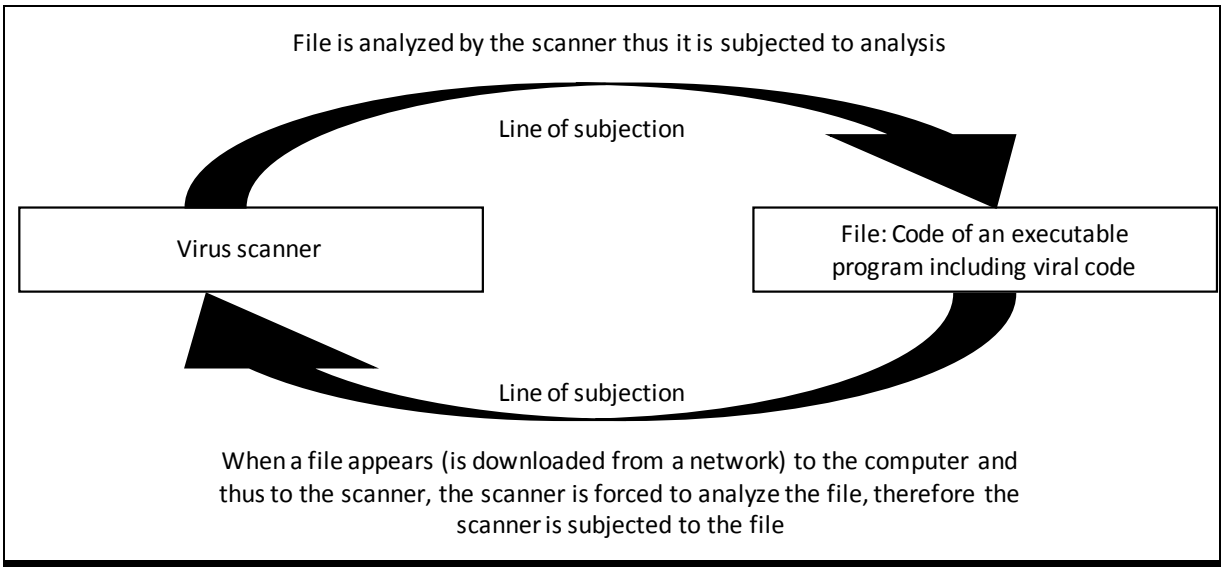

Figure 2. Connection and Subjection of Virus Scanner and a File with a Virus

2.2. The Emerging Connections

The security machine is not isolated but is connected to other machine assemblages, such as science. If we look at the applications of security and its modes of thinking we notice that they stem from science, although not exclusively. There are new thoughts – at least modifications of thoughts if not novel ideas – that creep into the picture and alter the applications. Knowledge of biometrics and behaviometrics (see Nisenson, Yariv, El-Yaniv, & Meir, 2003; Statham, 2006) – which here represent science – can alter locks. The lock in the door could be replaced with a biometric or behaviometric lock, or these could be added as features to the lock to increase its defense. Again, because there is a connection, there is subjection as well. The lock is subjected to the knowledge and application of the lock. On the other hand, as the lock is actually implemented, it could itself be studied by researchers who will then add to the field of knowledge of, for example, biometrics or behaviometrics. This is to say that the security machine is subjected to concrete machines in it – for example, doors, walls, locks, virus scanners, firewalls, encryption programs – and more abstract machines such as science and concepts of value; that is, what is considered valuable enough to requires protection. Moreover, it is important to note that the security machine is subjected to all of its connections. In addition, if we recall the concept of the emergence of novelty in the case of connections, we can note that the security machine is in a constant state of change – a state of "becoming", in Deleuzian terminology – since, firstly, the connections are emerging all the time and, secondly, the machines at the other end of the connections are changing. Deleuze prefers to use the word becoming instead of being since nothing ever stays the same but is in a constant state of change (Deleuze & Guattari, 2004a; 2004b; Stagoll, 2005; May, 2006, p. 59).

In order to produce some analytical order and to aid conceptualization, the security machine can be seen as functioning at various levels: the physical, the technical, and the social. Throughout our paper, the levels should not be understood to be strictly separate because they are not isolated from each other. For example, technical equipment is physical as well as part of the social world.

Keeping the above in mind, we could take another look at Figure 1. Along with the door (Machine unit A) shown in Figure 1, the concrete walls, corridors, and fences reside on the physical level, and the technical equipment (Machine unit B, an electronic lock in Figure 1), such as firewalls, intrusion detection scanners, and security cameras, constitutes the technical level. The social level includes different discursive elements such as policies (Machine unit C in Figure 1), compliance deals, and general regulations for behavior (actions aiming to control behavior, such as information security training). Figure 1 shows Machine D, which combines all the levels. At this point, we understand a machine as a producer/interrupter or, to be more precise, a machine that produces through

interruption and has connections. The security machine appears on the concrete and discursive (social) levels. It is a meshwork of machines – an assemblage.

3. Territory

Information – defined as data – always lies in the physical space and carries a precise order that may be formulated as a series of numbers or letters, or that may be a picture, a blueprint, and so on. Because information necessitates a piece of the physical space, there is a territorial aspect embedded in the notion of information. For instance, a file on a disk requires a particular physical space for "magnetic imprinting", and written information demands a surface – a space – on which to be written. Spaces are hence invaded – territorialized – by the material expressions of information; for example, signs, digits, or diagrams. There is always a medium, an occupied material space, without which information cannot exist.

This leads to a situation where no actual information lies beyond the material world. When we turn our attention to the actual, we have to take note of its counterpart, the virtual. There is virtual information that can be retrieved from a data storage device to actualize it in new processes. Actual information is something that is here and present, while the virtual includes information that can be brought into the domain of the actual. A distant memory is virtual if it is not thought of but becomes actual as it is recalled. When the memory is recalled it changes because it is altered by the constellation of other information and experiences to which it becomes connected in the process of recall (cf. Deleuze, 1988; see also May, 2006, pp. 45–52). This means that we can have information that is not actual information but which has the possibility for it to enter the material world. Alongside the aspects of virtuality and actuality, time begins to play a role: information in the form of spoken words withers away as the sonic waves – the materiality of the spoken words – fade. There is always a time for information to be "pronounced", a moment of appearance, and this is eventually followed by a moment of withering (see May, 2006, pp. 45–52; cf. Foucault, 2003, pp. 114–116). Any medium is written at some time, and wears out over time.

For now we have two aspects to the appearance of information: the spatial and the temporal. There is still one aspect to consider: the order of the information (i.e., what it is that is written). With the order of the information, we refer to the way in which the information is organized. For instance, consider this text. If the letters were mixed up randomly, the text would not carry its original information. Information security is not, therefore, just about space and time, but about organization and the order of that particular space.

3.1. The Chaotic Outside

Territory plays a dual role in our view of information security. Every piece of information reserves a territory (space on a disk or on a piece of paper for instance); however, on the other hand, there are also territories – safe zones – that are established to protect information. For example, a locked door or a password-protected account represents a safe zone territory that surrounds the data territory. In other words, the security machine has to establish or deploy its activity in the space that it is designed to shield. It is the order of information and the space that the information occupies that are protected. These safe zones are, nevertheless, surrounded by uncertainty – the forces of chaos outside (cf. Deleuze & Guattari, 2004b, p. 333; Grosz, 2008, pp. 10–11, 47). Michel Serres (2007, p. 126) calls this type of chaos "noise". The phrase "forces of chaos" mostly refers to the banal movement of different particles. This chaotic movement is the beginning of everything, which includes order and organization (cf. Deleuze & Guattari, 2004b, p. 345). Grosz writes, in a Deleuzian manner, about how chaos gives birth to the fragile order that is life, a term that could easily be replaced with "a piece of information", which holds an order as well:

> *"In the beginning" is chaos, the whirling, unpredictable movement of forces, vibratory oscillations that constitute the universe. Chaos here may be understood not as absolute disorder but rather as a plethora of orders, forms, wills – forces that cannot be distinguished or differentiated from each other, both matter and its conditions for being otherwise, both the actual and the virtual indistinguishably. Somewhere in this chaotic*

> *universe, in a relatively rare occurrence, through chance, molecular randomness generates organic proteins, cells, proto-life. Such life can only exist and perpetuate itself to the extent that it can extract from the whirling and experientially overwhelming chaos that is nature, materiality, and their immanent forces those elements, substances, or processes it requires, can somehow bracket out or cast into shadow the profusion of forces that engulf and surround it so that it may incorporate what it needs. […] [T]here is something fundamentally unstable about both its milieu and organic constitution* (Grosz, 2008, pp. 5–6).

Therefore, in terms of information security, the order born from chaos – the piece of information – is in a fragile state; that is, in danger of slipping back into chaos. The chaotic forces of outside threaten to penetrate inside (Deleuze & Guattari, 2004b, p. 345). An example should make the discussion more concrete. A hard disk, assembled in a production line, constructed from pieces of material, and configured precisely, constitutes a functioning storage medium. Solid stability of performance is sought, but unfortunate breakdowns and accidents do occur; for example, laptops are sometimes dropped. The physical failure of a hard disk caused by an outside force poses a threat in terms of information security because it scrambles the order on the disk and, in the worst case, makes the data irretrievable. The organization of information is lost. Again, the world outside and its altering forces constitute the threat. However, there are safety measures such as free-fall detection systems inside laptops or self-monitoring, analysis, and reporting technologies (SMART) applied to new hard drives that are engaged against the forces of failure. For instance, the free-fall detection system is designed to avoid or reduce damage when the laptop is no longer in control but thrown into free fall. It is literally a struggle between the forces that aim to maintain the fragile order and any uncontrolled movement that may possibly overthrow that order. If a failure occurs, and the disk loses the battle against chaos, there are still plenty of measures that seek to restore the lost order. Data recovery programs and the restoration of backups seek to do the job of re-establishing that order. The battle is lost, but the aim is now to attempt to move back to a time before the failure.

So we have the forces of chaos whirling outside, which threaten to erode and destroy the order inside. In order to establish an inside against the hostile outside, a border, such as a wall, has to be created and, thus, a territory, a safe zone, born (cf. Deleuze & Guattari, 2004b, pp. 343–347). This line or frame creates a territory out of chaos (Grosz, 2008, p.11). Importantly, however, the inside cannot be created anywhere other than in the middle of the outside, and that, to establish it, elements and components of the outside have to be used.

3.2. The Wall

There is no territory without a frame (Grosz, 2008, pp. 11, 13). However, it requires quite an effort to divide, limit, and confine space and maintain the order of the inside. The security machine is, thus, a wall-erecting machine. It creates physical walls, fences, and doors that all reside on the physical level and are quite easy to understand as borders. In many cases, borders are announced with “placards” (Deleuze & Guattari, 2004b, pp. 348–350). In the case of companies, a logo or name on the building announces a border, the beginning of the territory. In terms of information security, standards such as ISO/IEC 27002 describe the function of physical security as setting barriers in order to hinder outsiders from getting in (Basik, 2008, pp. 60–63; ISO/IEC 27002, 2005; Rogers, 2006, pp. 13–14). In practice, then, physical security is understood quite literally as a method of setting obstacles or barriers – erecting walls and fences – to create security perimeters in order to establish safe zones. This is the frame of territory without which there would be only chaos (Grosz, 2008, pp. 11, 13). This division establishes a categorical difference between us and them, insiders and outsiders. Moreover, borders do not emerge merely on the physical level. Technical walls are also erected: a firewall is the most obvious of these kinds of walls. A firewall follows the most basic digital pattern: allow or deny, true or false, one or zero. A firewall either accepts or rejects the attempt at connection. The previously mentioned passage-control systems constitute a part of the technical level in which an electronic lock is a technical placard that announces the borderline between inside and outside. A pop-up window that requests a username and password is another border placard.

In addition to the physical and technical level, the social level includes walls, too. Compliance to standards, information security policies, and code of conducts about how to handle information erect walls that seek to keep information inside. When individuals leave the territory for good (for example, employees quit their jobs), they become outsiders, which comes with consequences: their passwords and user accounts are terminated, and keys – perhaps uniforms and name tags as well – are taken away. The border cannot be ignored. It concretely determines who the agent is: an insider or an outsider. As long as the information exists, the ex-employee, now an outsider, is still in the reach of the security machine. For example, the employee might have agreed to a non-disclosure agreement in which they promise that they will not reveal the information in their brain to other outsiders. At this point, we have to remember the dual role of territory: there are the valuable assets that carry inner order – data territory (e.g., a file on a disk) – and then there is the other territory – the safe zone – that contains the maintained order (e.g., an office with locked doors, a firewall on its server, or compliance deals with employees). However, the difference between the two is more a theoretical or hierarchical one: the one is set to serve the other. The safe zone territory is established and walled in to protect the other territory that is constituted by the order of information. To put it slightly differently, the security machine seeks to keep the order of the secured object by establishing an ordered and controlled zone around it (see Figure 3). Ontologically, both territories are keeping chaos out. However, in Figure 3, we see that the safe zone still appears as the forces of chaos to the data territory. Anyone in the order of the safe zone – in reach of data territory – could destroy the order of the data territory. The territories are simultaneously subjected to each other: the territory, like any entity, possesses a subjective force.

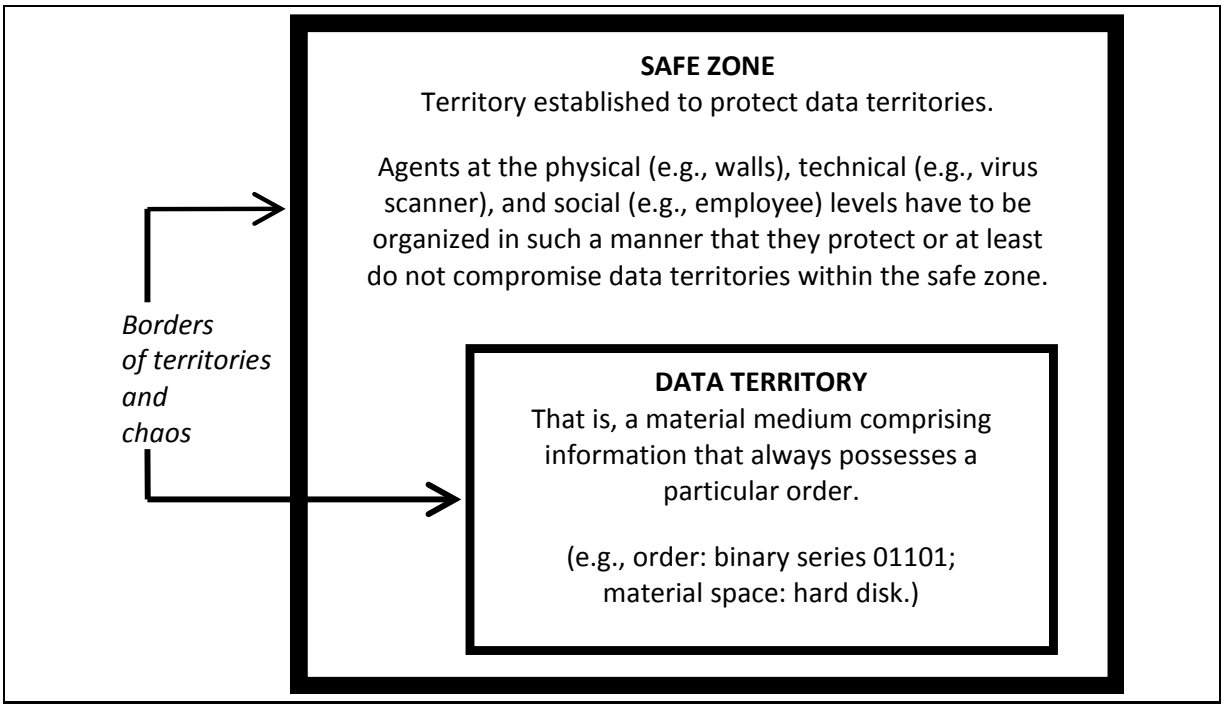

Figure 3. One Territory Inside Another

3.3. The Rhythms of the Inside

But what are the orders in the two territories? Again, it is a relational matter: if a secret is kept in a cellar (safe zone), then the order of the safe zone is constituted in the positions of the door and the lock. However, if we approach the issue of information security, it seems as though the order is based on CIA, which can be implemented through the use of identification, authentication, and authorization (IAA) (Dhillon, 2007). Nonetheless, we cannot emphasize enough that the machine possesses a virtual side as well: it is open to change. CIA/IAA is merely one way to carry out the task. Keeping

something safe in a hidden cellar is another way. Since CIA/IAA is a common feature of security machines, we have to consider what CIA/IAA means in terms of territory.

Let us first unpack CIA (confidentiality, integrity, and availability). On a practical level, "confidentiality" pertains to secrecy, which means that only selected agents can reach the information. This indicates that the physical space reserved by the information is confined or walled in. For instance, access to a file on a disk may be restricted through technical solutions. "Integrity" refers to the stability of the organization of data in that particular space. In our example, the file on the disk maintains its integrity if it does not get corrupted (integrity can be ensured through the use of checksums and backups).

"Availability" relates to accessibility: if the file is to be read, it has to be available. CIA can therefore be understood to concern the data territory. It relates directly to information, the space information occupies, time (when the information appears and how its material expression fades away), and the organization of that data. IAA (identification, authentication, authorization) provides a solution for what should be carried out to attain CIA. Nevertheless, we do not propose that the aim of CIA is reached if IAA is carried out. IAA is simply a proposal that many security machines have captured and connected to themselves. Furthermore, many measures have been developed that seek to achieve IAA. IAA does not relate to information as such, but it pertains to the safe zone territory that surrounds the shielded object. To seek IAA – to use practices that try to fulfill IAA – is a rhythm of safe zones. Deleuze and Guattari (2004b, p. 345) claim that a rhythm is an answer to chaos. Insiders at every level are made to function to this rhythm[4]. To become an insider is to begin to resonate with this rhythm. However, the complexity of the situation is apparent because IAA is just one rhythm of the inside. Compliance deals are not IAA, but involve control of the inside, which keeps information inside through social regulations. IAA is an important technical rhythm that leads to the idea of user accounts, which makes divisions in the territory. IAA organizes the inside. For instance, every user account has its own space that includes information that a user can access. This is basically territorial space management through the concept of user accounts. Borders are established against the outside world, but also against other users. Furthermore, users are not equal but are usually divided into hierarchical categories with different privileges.

Thus, territories deal with insides and outsides, and can be placed inside each other to give territories in territories. Furthermore, the situation is dynamic because territories constantly move in relation to each other. Attempts are made to keep the inside in controlled order, but there is constant movement in territories. A file can be copied, modified, and transferred. Still, there is a desire for hygiene – keeping the chaos out – on different levels: a virus scanner is responsible for keeping its territory clean (see Parikka, 2007), a door code seeks to keep outsiders outside, an information security policy tries to enforce the use of IAA when, for example, an unknown person requests confidential information, and so on. Because outside elements threaten the territory, the territory is placed under constant maintenance. For instance, walls and fences are fixed if they get broken down, and firewalls are updated, as are virus databases. Again, it is a question of the order of the inside.

[4] We find the term "rhythm" useful and descriptive. A rhythm is based on pulses, repetition, time, and timing. Take a moment to contemplate the following: how many repetitive tasks are there in the realm of information security, from the cycles of security update releases to the steady blinking lights of a firewall, from education sessions to awareness campaigns? How many times do you log in daily? Is there a cycle of maintenance of systems? Rhythms differ from one zone to another; still, the term captures a fair amount of the world. Moreover, as Deleuze and Guattari (2004b, p. 345) claim, this rhythm is an attempt to seal off the chaos outside. Here, the security machine expresses its productive side: look how much time we spend on information security.

Table 1. Information Considered as a Data Territory and Machine-Established Safe Zone

Data territory	Spatial	Order	Temporal
Appearance of a piece of information	Requires space in order to "appear"	Always carries a precise organization of order	There is always the moment of emergence
Example	A file on a disk	10010010	The moment when the file is created
Some possible forces of chaos (i.e., threats)	Unstable medium, cracker, natural disaster, a virus, etc	A virus scrambles the order to 10001000	Time wears out the physical medium
Example	A laptop is dropped accidently and the mass storage becomes damaged	The original order and thus the file becomes irretrievable	Information disappears at that moment
Rhythm of confidentiality, integrity and availability	(C) Only predefined users are granted access to the location or through networks	(I) The integrity is guaranteed, order remains the same or altered as desired	(A) Availability is ensured when the file is needed
Example	Administrator files cannot be accessed by a regular user	Checksums are calculated	At time 1 the file is available on medium 1, At time 2 - when medium 1 is out of order – the file is available on medium 2
Safe zone			
Appearance of a safe zone territory	Different types (technical, physical and social) of walls are erected in order to confine territory from the outside	Control of the zone is sought by organizing the order within	There is always the moment of emergence
Example	A firewall is installed, a compliance deal is drawn up, or concrete walls are erected	The firewall accepts only certain connections, the compliance deal seeks to organize and control the behavior of users, and concrete walls prevent outsiders from entering premises freely	The moment when the measures are put into effect and the duration of the measures
Forces of chaos (i.e., threats)	Something penetrates the physical space or the network of a safe zone	The control and the order of the inside is lost, if the inside is intruded upon	The force of becoming obsolete
Example	A virus, a cracker or a social engineer infiltrates the physical space or the network	Users do not comply but take mass storage devices out of the perimeter breaking the regulations intentionally on non-intentionally	A software run on a server becomes vulnerable to new viruses
One of the rhythms: identification, authentication, authorization	A user is identified (I) and authenticated as an insider by what they know (password), or how they appear (biometrics) or behave (behaviometrics). Users are authorized to access only certain spaces (physical spaces or files)	Everyone within the safe zone is under control as they have become insiders by going through IAA and complying with agreements	The status of being an insider as well as compliance deals both have duration
Example	A user enters a password, a fingerprint is scanned, or behavior is analyzed to allow access	Mass storage devices are treated as they should be according to inside regulations	An ex-employee is no longer an insider. A new employee is introduced to regulations

The categories in Table 1 should not be read as distinct because the dimensions of space, time, and order are tangled around each other. For example, if information disappears, this disappearance takes place in all the dimensions, and confidentiality relates to not only spatial but also temporal aspects as well. Furthermore, the table is illustrative – it is not a complete list.

4. The Volatile Agents – the Imported Chaos

4.1. Human Agents

The force of subjection is everywhere (see Section 3). In territories, all the agents throughout the levels are subjected to the order of the territory. On the other hand, the territory is subjected to these agents and their movements. For example, users go through IAA (in order to be able to log on to a system), but technical equipment is also configured – that is, subjected – to fit the system. As seen in the previous sections, the processes of taking in – the rituals of becoming an insider – are carried out on multiple levels. In other words, agents are shaped to belong to the territory: they are made insiders.

Nonetheless, the agents – even as insiders made compliant to the rhythms and practices of the inside – may pose a threat to the protected system. Throughout information security literature, the human element[5], as the users of information systems are labeled, has been postulated as one of the most challenging factors of information security (see Long, Wiles, & Mitnick, 2008; Mitnick & Simon, 2002; Schneier, 2004; Stanton & Stam, 2006; Winkler, 2005). Most security breaches occur due to the human element (Deloitte, 2007; Schifreen, 2006), whether intentionally or by mistake. For example, users may use weak passwords or not change them frequently enough – or users simply choose to ignore information security policies. Continuing the password example, the problem is dealt with quite easily using technical-level solutions: a system might automatically require frequent changes of passwords while simultaneously measuring the strength of the passwords suggested. Or to make it even more secure, the system could be altered to use biometric or behaviometric authentication measures in addition to the use of passwords (see Nisenson et al., 2003). Thus, the password would not play such a significant role because, if this method fails, another mechanism of IAA emerges. What the technical suggestions actually seek to achieve is (partial) removal of human agency. Humans are not programmable and, therefore, not easy to predict in comparison with rational machines.

The security machine functions at the level of ethics by seeking to create good users, good insiders, and good behavior in terms of information security[6]. The use of positive power (see Foucault, 1998, pp. 138–139) and creation of good users is required because rational and technical solutions cannot take over the entire field of human behavior. It should also be noted that the security machine is limited in space. This implies that the users in one security machine can be also users of another system, which may compromise the first system through incorrect behavior. For example, the security machine tells us – if it is effective in any way – that an employee should not use their passwords in any other system because, if the other system is malicious or leaks passwords, then every other system with the same password and the same user name will be compromised.

However, the creation of good users is far from being an easy task. What is uncontrollable with the human is the relation to the self. As Foucault (1992, p. 26) puts it, in the case of ethics, the individual has a relation to the self through an ethical code: the self is subjected by the individual to the code (see also Vuorinen, 2007). The code does not transfer directly but includes ways of carrying out the code (Foucault, 1992, pp. 26–27). For example, the rules implemented by the security machine usually seek to interrupt the flow of information to the outside, which prohibits the removal of flash drives to outside the perimeter. In subjection to the rules, human behavior is under double subjection:

[5] When we speak about the "human element" (and, in the next section, about technical agents) we note the same reservations as with the "levels". There is no pure human element; it is connected to the world of objects (Latour, 1993; 1999; 2005; Orlikowski & Scott, 2008). It could be even asked how the claim can be made that the human element is the problem in the world of information security, as this is an assemblage of humans and a system.

[6] Being a good user is to be aware of the security threats, which is to keep the system updated. Security awareness campaigns are an attempt to constantly remind the user of what good behavior – and thus being a good user – means (see Layton, 2005).

it is subjected to the rule and to the relation to the self. The question asking "what shall I do in order to comply with the rule" is the relation to the self that affects the behavior. In the end, will the employee go through their pockets thoroughly to discover possibly misplaced USB mass drives before leaving the office, or will they merely write the rule written on a post-it note? Or is the rule only stated in the written format of the information security policy book where it does not affect the actual behavior of individuals in any way?

The relation to the self complicates education, makes complying with information security policies more difficult, obscures the implementation of information security standards and frameworks – such as ISO 27002 (2005) and COBIT 4.1 (2007), and actually eludes them because the relation to the self lies almost beyond capture from the outside. From the viewpoint of information security, the double connection is an outside element that is imported to the organized territory. It is chaotic, unpredictable; it is noise (see Serres, 2007, p. 126) – an example of the forces of chaos that stem from the outside. In addition to this double subjection, the users import chaos to the inside in the form of thoughts that relate to the outside. From thinking of anything that is not work related to idling on social media sites (such as Facebook, YouTube, or Twitter), this is a manifestation of the outside, the chaos.

4.2. Technical Agents and the Whirling Outside

Chaos at the human level is evident and chaos "contaminates" technical systems through users. However, technical equipment, even though it is used as an order-bringing element, carries with it its own unpredictability. The technical level harnessed to the security machine is neither pure nor without flaws. Despite quality checks, integrity checks, and self-diagnostics – which are themselves security machines – faulty products are connected to the security machine. Technical-level products wear out, include bugs, and may be exposed to malware. Even without any errors, the technical level is brought from the outside and, because it is connected to the inside, might not be compatible with the internal order. This is the reason it might be better not to install updates immediately after release (Beattie, Arnold, Cowan, Wagle, & Wright, 2002).

What is important to note here is the fact that everything within the territory is brought from the outside, which the territory is also fighting. In other words, there are no "inside elements" as such; they all originate from the outside and, through rituals, such as IAA, elements become insiders. As discussed in Section 3, the inside has to be established in the middle of the outside, and now we see that all the elements – the machines which are finally inside – are brought in from the chaos. Everything from operating systems to virus scanners, firewalls, security standards, frameworks (e.g., ISO 27002, 2005; COBIT 4.1, 2007), and updates are imported from the outside.

In summary, the territory is a region in which the order is arranged by the security machine. However, it is not a total blockage – an isolated isle in the sea of threats. Information has to be available when needed and, thus, the machine is filled with movement: movement that is allowed to enter the territory. Data packets rushing into the network represent this kind of movement. The particles that are moving – whether human, technical, or physical – originate from the outside. It is like folding a page in a book: an inside is created in the fold – the pleat – but this stems from the book, the environment (cf. Deleuze, 2006; Grosz, 2001, p. 68; Serres & Latour, 1995, pp. 59–62). Through the machine and territory metaphors, we can realize that information security is a machine-filtered and machine-ordered territory, which is "folded" from its environment as an intensive mesh of connections. In Table 2, we present some of the outside effects that take place in the territory. Again, this is not intended as a complete list; the table is only intended to be illustrative.

Table 2. The Imported Chaotic Outside

	'Natural' flaws (before implementation)	Measures of prevention	Flaws generated within after implementation	Counter measures	Problems in connection	Counter measures
Technical level	Faulty circuits, bugs in program	Quality checks, alpha and beta testing	Product wears out, becomes vulnerable to new malware	Replacement, updating software	Product turns out to be incompatible with the new environment	Re-couplings, removal of the product
Social level	Employees, people who are usually unknown previous to recruitment, possibly not trustworthy Information security policies may possess faults	Interviews, background checks (from available registers) Updating and tailoring security policies accordingly	Double subjection (there is the relation to the self between the behavioral code and the self)	Molding, education, further technical-level solutions	Not a good user, that is, transfers uncertainty to technical level with careless use	Technical-level solutions, continuous education Managerial solutions (punishment for bad behavior, warnings and dismissal if compliance refused)
Physical level	Uncertain structures of material or undesired elements come with it (e.g., dust)	Quality checks, guards, reception desks	Material wears out, locks rust	Replacement, continuous checks, cleaning rooms	Interrupts correct flows	Removal, re-coupling

5. Discussion: Implications

At this point, we understand the role of information security as an interrupter. In other words, the security machine comes between two entities such as a threat and a protected object that resides in an information system. Therefore, information security – the security machine – is always the third entity, the third agent that is included in the system in addition to the user agent and information. In practical terms, information security is always invited into the system from the outside as a third entity, whether it comes in the form of a firewall, information security standard or framework, information security policy, or an employee that carries out a security-related task as part of the security machine (Cf. Serres, 2007, pp.187–188). Thus, information security is a parallel addition to a system – even in cases in which security is integrated in the design of the system (cf. McManus, 2009; Siponen, Baskerville, & Heikka, 2006). In brief, information security is part of the outside for which inclusion in the system is sought, while for some other chaotic parts – information security threats – exclusion is sought; an entity is included in order to gain the ability to exclude. For example, a virus scanner is invested in, brought in from the outside, in order to give the information system the ability to exclude malware.

However, after the security machine is integrated into the system, it transforms the order of the system. In other words, a system with the addition has a more complicated order than one without it (Serres, 2007, p.188; see also Figures 1 and 2 in this paper). Now there are two orders: the order of the original system and the order created through the security machine. Nonetheless, these two different orders represent chaotic noise to each other as the need for reciprocal adaptation emerges: they are subjected to each other (see Figure 2). Furthermore, the entire apparatus – the constellation of systems, its users and information security machinery – has become something different: it has been transformed through the process of emergence described in Section 2.2. What is gained in such a situation from the system's point of view is the improved chance to achieve CIA (an open system would be overrun by the outside chaos). However, the cost is increased complexity.

As we demonstrate in Section 2, information security works through interruptions. However, only a small proportion of the interruptions are directed toward attacks from the outside. Instead, the object of the security machine's activity is for the most part the inside. Here, it is important to note that the

security machine's way of functioning is interruption. That is to say that information security primarily interrupts the inside when it comes between the user and their work in the form of awareness campaigns, password changes, locking computers, software security updates, information security education, regulations, locked doors, the use of keys, and so on (see Figure 3). However, we want to emphasize the fact that information security can also connect and mediate through interruption (for example, private email systems interrupt users by requiring a password, but this interruption is necessary for the existence of privacy).

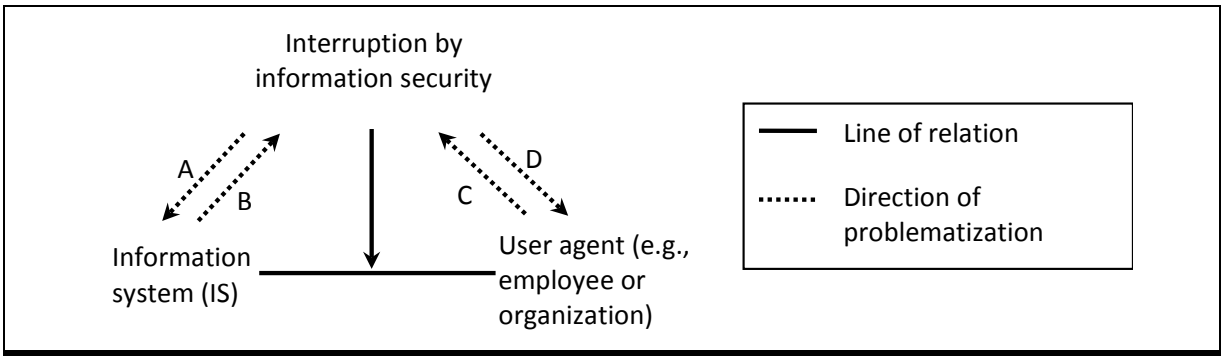

Figure 4. The Relationships between Information Security, IS, and User Agent, and the Direction of Practical and Research Problematization

The direction of problematization represented in Figure 4 by line A is widely known: this represents the problems information security causes to the system; for example, the processing power that information security requires, or the effects updates have on the stability of the system. Line B represents the view by which the system itself is seen as a security problem. For example, different operating systems are considered to contain different security problems, so the design of the system might be a possible source of problems (e.g., McMagnus, 2009; Siponen et al., 2006). Furthermore, security standards, frameworks, and best practices consider information systems as problematic, and list dos and do nots for how to overcome and avoid these problems (e.g., ISO 27002, 2005). Line C represents the view of users and organization as problematic. The social side of information security approaches this problem by asking, for example, how to make users obedient to security norms and what the best way to educate them would be (e.g., Karjalainen & Siponen, 2011). The repeated argument that the human is the weakest link (e.g., see Long, Wiles, Mitnick, 2008; Mitnick & Simon, 2002; Schneier, 2004; Stanton & Stam, 2006; Winkler, 2005) is included in Line C. Line D has not been at the center of information security research and has remained mainly unexamined.

What, then, is there to study in terms of line D? Line D is the problematization of information security but not from the point of view of improvement. It represents questions such as "how is information security problematized by the users and organization?". More generally, because information security is not a neutral entity but rather an interrupting and producing actor, we should study the effects of the security machine on the user agent and organization. Moreover, we should examine what is interrupted in various situations – what relations are broken by the activities performed by information security, the security machine. Other questions for investigation include how information security co-exists with us (what requirements it places on us, for example, in terms of updating; what do we have to do – wait, install, restart the computer?), how it stays parallel to us (how it is always between the user and the machine; what effects this has on the user), how we are connected to it (how we are driven by the security machine to behave), what we are coupled to (all the information security measures we are subjected to), and what kind of machine we become. There is also the moral side to consider – for example, what kind of moral obligations come with the security machine? If a computer is infected by malware, where do we place the moral blame? We live with, in, and parallel to security machines. Our information is circulated through them. How do they change our territories, how are we subjected to them, and how do we become part of the subjecting machine? What do we become as part of it? What is the rhythm that comes with the coupling? For example, if an organization implements a standard, in what concrete situations does it actually place users on a regular basis?

For instance, what are the educational updating cycles? Can information security be so closely coupled with our life and have such an impact on us, on our organizations and territories, and yet be taken as a given so that it is almost invisible to us even though we live in and with it? The fundamental question is what else the security machine produces besides the order it seeks. In other words, what does it concretely mean to carry out security measures? As an addition to our life, what noise and chaos does it bring about? Briefly, we suggest that we should pay attention to the ramifications of being a part of and subjected to the security machine. In order to carry out this task, we have presented concepts relating to the security machine – interruption, coupling, subjection, emergence, territories (safe zones and data territories), inside/outside, order/chaos, walls and the spatial examination of information, CIA and IAA – to bring some conceptual order and provide a starting point.

6. Conclusion

We argue that information security is, ontologically, an order-preserving and producing socio-techno-material machine that is a multiple, connective, territorial, subjecting, and transforming interrupter and producer. The security machine harnesses and subjects agents so that the combination created is able to carry out its task of interrupting chaos. Information security is an order-maintaining rhythm machine. Its main goals are to maintain the order of information written on a medium, and to maintain the order of surrounding territories – the safe zones. The constant becoming – the emerging connections and disconnections of the machine and its targets – makes the entire constellation transformative, which may send this precious order back to chaos.

In the task of creating an order inside the system, information security interrupts the agents inside. However, the security machine is not a mere interrupter but a mediator. It makes the outside and chaos relevant to the order of information. Through passwords and user names, the security machine produces a relation between the system and its users. The security machine is all about the purification of the outside and the organization of the inside. The aim is for chaos to be left outside and the elements brought inside to be purified. However, there is always noise: while information can theoretically be pure at the level of order, it can never be pure when it is written on a medium because the noisy material medium becomes part of the information. An inside cannot be completely purified because it is built out of elements of the outside; the only difference between the elements lies in their order and organization. Information security is an order itself, but it is not without impurities. Chaos gets in. In fact, chaos is invited in by the security machine, which itself comes from the outside as an addition to the information system. As information security is an active entity, we propose that its effects on other agents inside the system should be studied. In this paper, we introduce concepts that could be used in such research.

References

Basik, S. (2008). *Building an effective information security policy architecture*. Boca Raton, FL, USA: CRC Press.

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

Beattie, S., Arnold, S., Cowan, C., Wagle, P., & Wright, A. (2002). Timing the application of security patches for optimal uptime. *Proceedings of LISA '02: Sixteenth Systems Administration Conference, USENIX* (pp. 233-242).

Bennett, J. (2010). *Vibrant matter. A political ecology of things*. Durham, NC, USA: Duke University Press.

COBIT 4.1. (2007). *Framework, control objectives, management guidelines, maturity models*. Rolling Meadows, IL, USA: IT Governance Institute.

DeLanda, M. (2009). *A new philosophy of society: assemblage theory and social complexity*. London, England: Continuum.

Deleuze, G.. (1988). *Bergsonism.* New York: Zone Books.

Deleuze, G. (2006). *The fold: Leibnitz and the Baroque*. London: Continuum.

Deleuze, G. & Guattari, F. (2004a). *Anti-Oedipus: Capitalism and schizophrenia.* London, England: Continuum.

Deleuze, G. & Guattari, F. (2004b). *A thousand plateaus: Capitalism and schizophrenia.* London, England: Continuum.

Deloitte. (2007). *2007 global security survey: The shifting security paradigm*. London: Deloitte.

Dhillon, G. (2007). *Principles of information systems security: Texts and cases*. New Jersey, USA: John Wiley & Sons.

Dhillon, G. & Backhouse, J. (2001). Current directions in IS security research: Toward socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153

Foucault, M. (1991). *Discipline and punish: The birth of the prison*. London: Penguin Books.

Foucault, M. (1998). *The will to knowledge: The history of sexuality volume 1*. London: Penguin Books.

Foucault, M. (1992). *The use of pleasure: The history of sexuality volume 2*. London: Penguin Books.

Foucault, M. (2002). Subject and power. In J. Faubion (Ed.), *Power: Essential works of Foucault 1954–1984 Volume 3* (pp. 326–348). London: Penguin Books.

Foucault, M. (2003). *The archaeology of knowledge*. London, England: Routledge.

Grosz, E. (2001). *Architecture from the outside: Essays on virtual and real space*. Cambridge, MA: MIT Press.

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

ISO/IEC 27002. (2005). *Information technology – security techniques – code of practice for information security management*. Geneve: The International Organization for Standardization.

Karjalainen, M. & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555.

Latour, B. (1992). *Where are the missing masses? The sociology of a few mundane artifacts.* Retrieved from http://www.bruno-latour.fr/sites/default/files/50-MISSING-MASSES-GB.pdf

Latour, B. (1993). *We have never been modern*. New York: Harvester Wheatsheaf.

Latour, B. (1996). On actor-network-theory: A few clarifications. *Soziale Welt, 47*(4), 369–381.

Latour, B. (1999). *Pandora's hope. Essays on the reality of scientific studies.* Cambridge, MA:Harvard University Press..

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

Layton, T. P. (2005). *Information security awareness*. Bloomington, IN: AuthorHouse.

Long, J., Wiles, J., & Mitnick, K. D. (2008). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing.* Burlington: Syngress.

McManus, J. (2009). Security by design. In A. Oram & J. Viega (Eds.), *Beautiful security. Leading security experts explain how they think.* Sebastopol, CA: O'Reilly.

May, T. (2006). *Gilles Deleuze: An introduction*. New York, USA: Cambridge University Press.
Mitnick, K. D. & Simon, D. (2002). *The art of deception: Controlling the human element of security*. Indianapolis: John Wiley & Sons.
Nisenson, M., Yariv, I., El-Yaniv, R., & Meir, R. (2003). Towards behaviometric security systems: Learning to identify a typist. *Proceedings of the 7th European Conference on Principles and Practie of Knowledge Discovery in Databases* (ECML/PKDD) (pp. 363–374). Berlin, Germany: Springer.
Orlikowski, W. J., & Scott S. V. (2008). Sociomateriality: Challenging the separation of technology, work and organization. *Academy of Management Annals*, *2*(1), 433–474.
Parikka, J. (2007). *Digital contagions: A media archaeology of computer worms and viruses.* New York: Peter Lang Publishing.
Pieters, W. (2011). The (social) construction of information security. *The Information Society*, *27*(5), 326–335.
Pyyhtinen, O. (2010). *Simmel and 'the social'*. Basingstoke, England: Palgrave Macmillan.
Rogers, M. (2006). Internal security threats. In H. Bidgoli (Ed.), *Handbook of information security: Threats, vulnerabilities, prevention, detection, and management* (Vol. 3, pp. 3–17). Hoboken: John Wiley & Sons.
Schifreen, R. (2006). *Defeating the hacker: A nontechnical guide to computer security*. New York: John Wiley & Sons.
Schneier, B. (2004). *Secrets and lies: Digital security in a networked world.* New York: John Wiley & Sons.
Serres, M. (2007). *Parasite*. Minneapolis, MN: University of Minnesota Press.
Serres, M., & Latour, B. (1995). *Conversations on science, culture, and time*. Ann Arbor, USA: The University of Michigan Press.
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), 725–770.
Stagoll, C. (2005). Becoming. In A. Parr (Ed.), *The deleuze dictionary* (pp. 21–22). New York: Columbia University Press.
Stanton, J., & Stam, K. R. (2006). *The visible employee. Using workplace monitoring and surveillance to protect information assets – without compromising employee privacy or trust*. New Jersey: Information Today, Inc.
Statham, P. (2006). Issues and concerns in biometric IT security. In H. Bidgoli (Ed.), *Handbook of information security: Threats, vulnerabilities, prevention, detection, and management* (Vol. 3, pp. 471–501). Hoboken: John Wiley & Sons.
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), 27–38.
Winkler, I. (2005). *Spies among us. How to stop spies, terrorists, hackers, and criminals you don't even know you encounter every day.* Indianapolis, IN: Wiley Publishing.

About the Authors

Jukka VUORINEN is a sociologist and doctoral student in the Department of Social Research at the University of Turku, Finland. In terms of research, he is intrigued by the social aspects of information security. His research interests vary from the world of software crackers and the culture of copy-protections to the ontological questions of information security. The most influential element concerning his academic thinking has been the Foucault circle. This eight-year-old reading group was founded by him and his colleagues around Michel Foucault's texts in order to study and discuss Foucault's oeuvre. Later, as there was nothing left to read by Foucault anymore, the group was forced to expand beyond Foucault to Gilles Deleuze, Michel Serres, Elizabeth Grosz, and Jane Bennett.

Pekka TETRI is a Ph.D. candidate in the Department of Information Processing Science at the University of Oulu, Finland. He holds a Masters' degree in Information Systems Science. His research topic is social engineering – the human factor in information security. He spends most of his time as a practitioner with expertise in counter HUMINT, counter surveillance, information security management, social engineering and employee behavior. Pekka is currently located in Espoo as both Ph.D. candidate and practitioner with his wife Laura, daughter Mathilda and son Kasper, who are the source of his inspiration.