Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2009 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Fall 8-11-2009

SECURITY AS A MACHINE - STRUGGLING BETWEEN ORDER AND CHAOS

Jukka Vuorinen
University of Turku, Finland, juanvu@utu.fi

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

SECURITY AS A MACHINE – STRUGGLING BETWEEN ORDER AND CHAOS

Jukka Vuorinen
Department of Sociology
University of Turku
20014 University of Turku, Finland
jukka.vuorinen@utu.fi

Pekka Tetri
Department of Information Processing Science
University of Oulu
90014 University of Oulu, Finland
pekka.tetri@oulu.fi

Abstract

Our intention is to use Deleuze and Guattari's concepts of machine and territory to place the classical notion of information security in a new light. In other words, we seek to describe how information security appears if confidentiality, integrity, and availability (CIA) and identification, authentication, and authorization (IAA) are considered to constitute part of a dynamic security machine. Moreover, not only information itself but also CIA and IAA are seen differently in the light of the machine concept. What is information security if it is thought of as a machine, and what is it that it does exactly? How does information security function in different environments? Instead of focusing on individual security patterns and safeguards, a collection of do's and don'ts, a fresh perspective at a higher level of abstraction brings about a novel viewpoint on security.

Keywords: Security machine, Information security, Territory, Dynamic security.

1 INTRODUCTION

Over the course of the years, a large number of problems have been constructed within the world of information security. These problems have germinated other problems and solutions as well. Some examples of these are: does gaining access to a mainframe automatically confer permission to use that mainframe – in other words, is locked-door protection enough (the problem of access)? What if there are multiple individuals using a computer – is it possible to lock some of the files in the computer (emergence of accounts)? If passwords are the solution to the question 'how do we identify users', then we have another problem of proper passwords. What about when users forget them? What constitutes a proper password?

These are all questions that are very familiar to anyone who has worked within the information security field. Moreover they are so self-evident that they are almost invisible. We tend to forget that there could have been other problems and solutions, as the notion of confidentiality, integrity, availability (CIA), and identification, authentication, authorization (IAA) – the idea of how security works – has become the norm and the starting point of thinking. Often issues within information security are faced as problems that require a solution. There is nothing wrong with this, but usually when an answer is sought for a problem, whole networks of threads and connections are not seen, if problems and solutions are dealt with separately. In other words, setting everything within the framework of 'problem/solution' fails to take into account connections that are not immediately related to the problem. We are claiming, in this paper, that if we think of security as a transforming, absorbing, connecting and disconnecting machine (not a static mechanism), we can reach a picture that reflects security in a novel way. Furthermore, it will not be simply an abstract painting of how things mysteriously move; the attempt is to show the connections and moves at a very concrete level as well. If we can reach this picture, we can ask questions a little differently, in order to see connections and relate problems in a new way. By making the connections of information security visible, we are able to explore new relations such as the relation between value and information security. An analysis of the components, such as firewalls, policies, cryptography and investments, becomes possible. By sketching the big picture with a new way of thinking, we can see the dispersion of the security thought and practices. We would like to present a way to think about security and to approach its fundamental questions from a different point of view. What is it exactly that security does? How does information security function in different environments?

First we set the scene by introducing the notion of the 'machine' that has been developed by the two French philosophers Gilles Deleuze and Félix Guattari. We apply the concept of the machine to security, and present a theoretical division in the three levels of physical, technical and social, trying to depict the ways in which the machine connects and disconnects. As the focal concept is sketched out, we turn to its source of power. We argue that the machine is largely value driven and we seek to demonstrate the position of value in information technology and security. The fourth section discusses another of Deleuze and Guattari's concepts: 'territory'. We claim that the security machine creates territories, and that the machine simultaneously shows its spatial and temporal side: information requires a physical space and time in which to appear. The abstract security machine functions in the material world of space and time. We try to capture relations between the inside and outside of territories, the order within and the chaos outside. In addition we place CIA and IAA within the concept of territory.

The security machine is very much concerned with practices, and thus the fifth section explores the relationships between agents inside territory under the regime of the security machine, which creates subjects of inside: the machine approaches users and employees, and this has consequences. In the end, before we go into our conclusions, we try to present dysfunctions of the machine by analyzing the concept of the firewall thought on which the machine relies. We consider how things go wrong and why territories leak information.

2 SECURITY AS A MACHINE

French philosophers Gilles Deleuze and Félix Guattari (2004a) created the concept of a 'machine'. For us, it provides a metaphorical tool for use in considering security and information security in a novel manner. As the concept is applied, it opens up a viewpoint that describes aptly the scene of security and helps in understanding the security activity as a whole. Although we are using the machine metaphor as a methodological tool, the security machine exists materially and has concrete ramifications. These claims – obviously – require careful analysis, which we intend to present in this paper. The first task is to outline what the machine is. Deleuze and Guattari (2004a, 2, 5–6, 38–39) claim that a machine has a function, which is to produce and interrupt. They bring up an example of a mouth as a machine (Deleuze & Guattari 2004a, 39). It can produce, for example, a flow of chewed food to stomach. In the same way, in terms of physical security (which is also part of information security), a door is a machine. It forms a barrier between in and out. As a door produces a temporary hole in the wall, it carries out an enormous task; without the door, there would only be a wall, through which it is much more difficult to enter or exit (Latour 1992, 154–155). The stream of individuals arriving and departing flows through the temporal hole – the door. It is a machine producing the flow, a flow that is also interrupted by the same machine when the door closes. As demonstrated here, a machine can be anything that merely interrupts a flow of something – chewed food, a crowd, or information security, as we intend to show in this paper.

These Deleuze-Guattarian machines do not stand isolated but become connected, forming huge assemblages. Deleuze and Guattari (2004a, 5) actually state that a machine is always a part of 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, 39). Referring again to the physical side of information security, a door is not an isolated machine carrying out its job. A corridor connected to the door is another machine that creates lines of movement, allowing a spatially confined stream. The limited space between the walls prevents (interrupts) the chaotic dispersion of 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 more traditional machines. In fact, the door can have multiple points of connection; it may be connected to a logger that in turn forms a connection to an information system. This is to say that a door is connected, in a direct way, to a network of other agent/token-hybrids and machines that form part of a security machine at a single level in space. This also implies that there can be different levels of abstraction. A door denies and allows entrance, divides and creates territories (with the help of walls, fences, surveillance and other agents) while at the same time providing information about those who pass via loggers (connected to information systems). Thus, a door as such is connected to other machines, and depending on what it is producing, it has several layers of function, production, in different individual levels within the space of the security machine. For instance, a link can be established between a door and a passage control system that logs – produces lists of identifiers of – people's entrance to and exit from the building. The logger is in sync with the door in which it is embedded. This new machine – the assemblage of the door and its control system – connects to machinery that produces security through the set of interruptions. This is the security machine that spreads like a rhizome through various levels: the physical, the technical, and the social (cf. Deleuze & Guattari 2004b, 7). The concrete walls, corridors, fences and doors reside on the physical level, as the technical equipment, such as firewalls, intrusion detections scanners, and security cameras, constitutes the technical level. The social level includes different discursive elements such as policies, compliance deals, and general regulations for behavior (rules that forbid the taking home of flash drives and so on). Nonetheless, the division of the machine into the three levels is merely a theoretical move, which makes the machine formed by security more visible and opens up an opportunity for analysis. It is important to note that the machine rarely appears on one level only. The door (on the physical level) can be connected or embedded to the technical level as in the case of the logger, and the assemblage of door and corridor takes place on the physical level. In addition it is a social-level event as individuals meet the door. There are socially regulated rules on how to pass through the door (preferably with clothes on, through a certain door for a certain situation, etc). There are also policies

regarding the door: an authorized person must pass through the door alone. This is to prevent piggybacking (or tailgating), so that a person without permission cannot immediately follow behind an authorized person while the door is still open. It is also worth noting that in this example, the policy applied seeks to override what is considered common courtesy: holding the door for a stranger is not permitted according to this policy.

The security machine is actual – present – when it is deployed, when activity is carried out, executed. However, there is also a virtual side to the machine, meaning that the machine stands open to change since it can connect to anything (cf. May 2006, 47–50). As seen above, there are infinite numbers of concrete connections that a part of a security machine can create, and it is difficult to foretell what the connections will be like in the future. The machine is dynamic and novel in establishing new connections but not only on the concrete level (cf. Deleuze & Guattari 2004b, 7, 232). Michel Foucault (2003a, 44–54; see also 1991; 2003b; 2004) writes at various points about how an object (for example a prison, madness) requires a certain constellation of statements, discourses and episteme for it to surface. Information security – considered as an object – is no exception, but requires preconditions, first, to surface, and later, to develop. Keeping this idea in mind, knowledge begins to play an important role. We can ask questions such as with what constellations of knowledge objects become possible, or under what conditions objects emerge: the literature and journals of information security excavate strata of knowledge, creating a new knowledge sediment, namely, the view of information security as science. Science does not arise from a void; knowledge sediment as well as praxis underneath and preceding it creates the constellation from which it surfaces. Knowledge of algorithms, cryptography, and behaviometrics, as well as methods and paradigms used by other branches of sciences pave the way for information security as science. (Cf. Foucault 2003a; Deleuze 2006, 41–58.) In information security terms, best practices are sought. The machine can harness anything that contributes with the protection mission of the security machine. Practices are constantly tested and developed in studies which vary the elements of a machine that is in state of becoming[1] and transformation. New connections emerge while others wither away. For instance, the concept of a username and password has prevailed for some time, but in the future this may be entirely replaced by bio- or behaviometrics. Still, it should be noted that the previous ideas are based on the concept of a user and an account; all the previous solutions seek an answer to the problem of identification and authentication. The two (identification and authentication) become inseparable in this categorical thought which confines the solution, and this is the argument we would like to emphasize. All in all, security machines are open to change and new connections on both the concrete (physical connections) and abstract (harnessing and applying new knowledge) levels. Briefly, the security machine can absorb and bend elements that have been used elsewhere; it reacts to its environment, whether due to a security solution or to a new threat. A very concrete and banal example is provided by software security updates that are reactions to changed situations (i.e. a new threat in the form of malicious software or a newly-detected bug in the software).

At this point we understand a machine as a producer/interrupter, or to be more precise, a machine produces through interruption, and has connections. The security machine is an abstract machine that nonetheless appears on the concrete (physical, technical) and discursive (social) levels. It is a meshwork of machines. Some of the machines can be sub-machines to others, but it would be a mistake to consider the constellation of machines as a hierarchal one, or as a single central machine. It is a net of relations that is formed out of tiny pieces, and occurs in practice. It is a complex set. Some parts of the network may have more connections attached to it than others.

What the security machine does is it – more or less gently – guides its subjects. 'Subjects' refers, here, to the agents that lie under the regime of the machine, including every agent on the physical, technical, and social levels. Agency thus can be possessed by any concrete object – it does not require an intentional subject (i.e. Latour 1992). A door is, therefore, a subjecting agent within a security machine. People coming in and going out are subjected to the door. As mentioned before, it is rather

[1] 'Becoming' refers here to constant change, 'multiplicity' (see Deleuze & Guattari 2004b, 38; Grosz 2005, 17; May 2006, 59-60).

difficult to walk through walls: this is the point of guidance, of how the door subjects and guides. We have to put an emphasis on positive productive power instead of negative and repressive power (see Foucault 1998, 136): the door is not so much coercive as it is temping, as it gently provides a point of entrance. It is also important to note that it is not only intentional agents that are subjected: the subjected agent may take the form of a firewall or a concrete wall. To configure a firewall is to subject it. To guide people to use a door is to subject them. To build a wall is to subject it. To face a dead end (a wall) is to become subjected by it.

The machine metaphor provides a broad viewpoint on information security, in which no one possesses the power; it always lies somewhere in between. The door holds a position, but still an individual has the choice to enter or not, to break through a wall or not. A wall cannot simply be erected anywhere, for example in the middle of a highway. In other words, walls are also subjected: to laws, erosion, graffiti artists, etc. A wall has a function that is not to coerce but to tempt, and agents – such as forces of nature or graffiti sprayers – do not always 'respect' it. Thus, the security machine is not about forcing but positive and productive power, which refers here to guidance – in other words there is an attempt at increasing productive assets (cf. Foucault 1998, 136). In this way, the machine metaphor also provides a connective aspect, showing that it is not the case that everything is in the hands of one individual; rather, it is a question of a complex situation in which strings are pulled from multiple positions. The functioning of the security machine is based on a constant stream of rationales which refer to reason and rationality. One of these rationales is the desire for value growth.

3 VALUE

Value is a system-level property, not an object-based one. Furthermore, it can be argued that information security is driven by value, which is derived from systems of desire. For example, a know-how secret is a valuable object – a valuable asset – in the business world since it provides the means to generate profit. As we know, profit is pursued in the business world, thus in this sense it is logical and rational to keep the secret which will pave the way to profit well-hidden. Ensuring profitability by securing the secret becomes a task for the security machine. In a sense, value assigns the job to the machine or calls (initiates) the security machine. However, it is also known that not all valuable objects are placed under protection; not all objects are understood as valuable ones. For example, a social engineer can benefit greatly from the company directory in order to impersonate an employee (Mitnick et al. 2002). Conversely, a list of names, titles and phone numbers can be regarded as worthless by a company. This relates to the problem of how value is constructed: value is a system-based property. If someone is about to break into a company by stealing the identity of an employee, it is useful for them to have a listing of employees. Therefore the listing possesses functional value; it may not be valuable in itself, but when it is brought into a particular context, its functional value can be understood. If objects can be utilized to achieve particular goals, they possess value. This is to say that value may be constructed relatively; it is possible to generate value in a system of relations depending on what the function of the system is. If a system – such as economics – seeks to profit, then everything inside the system contributing towards this goal is considered valuable. To put it simply, if something is valuable, this may be enough to initiate protective activity or, at least, it would be understandable and rational to summon protective machinery.

It may seem as if there was also a 'subjective' level on which value is generated. An email message from a passionate lover could be the most valuable object in the world for the recipient. As we argue that value is the initiator of security machine, in this case the recipient may initiate the security machine by creating multiple backup copies, in an attempt to ensure that the mail is never lost. But is this merely a subjective-level experience? In fact, there is not merely a subjective level involved here, but cultural influence also plays a part – and why not biological influence too – since this situation requires a particular conceptual frame for romance that is not universal and is bound to a specific moment in history. For instance, the ancient Greeks experienced 'sexuality' very differently (Foucault 1990; 1992). In any case, it is very difficult to realize what is valuable since the value is *placed* on the object rather than being essentially within the object. Perhaps a more banal example of relations – and hence systems – is provided by oil. Oil in itself is not valuable, but when there are millions of

combustion engines in the world, oil-based heating, and so on, its value becomes apparent. The value is created not just by the existence of combustion engines but by the will (desire) to use them. Again, the value does not lie within oil – there is no valued 'essence' of oil as such – but is placed on it in a system of relations. Moreover, an object can have value that derives from several systems. Niklas Luhmann's (i.e. 1989, 15–21) theory on systems and communications states that every system has its own code through which it communicates and to which it resonates. For instance, the code for the system of law is legal/illegal. This is the code of legal evaluation, which does not use political codes, aesthetic codes, or economic codes, but resonates only on the axis of legal/illegal. However, objects usually become defined by multiple systems, and thus there are plenty of sources from which value can arise: a work of art may be defined in terms of aesthetics, based on whether the work is appreciated, whether it is beautiful, and on what basis these questions are judged. In addition, the work of art may also be coded in terms of ownership: who owns the piece of art and what price (value) might it possibly reach in an auction. Furthermore, the legal system resonates around the question of who is permitted to sell it, while the political system could define the work as a national treasure (of national value) and regulate it by legislation in such a way that exporting it could be impossible. Still, it could be argued that having numerous aspects and viewpoints on an object is not a new idea. What is remarkable about Luhmann's theory is that a system considers surrounding systems merely as a chaotic environment which can be understood (has order) only if the environmental communication resonates with the code of the system (Luhmann 1989). This could be translated to the machine viewpoint, in which machines that pursue profit seek connections to machines that will feed power into them, and into the production of profit. The Luhmannian resonance – the 'reaction frequency' of a code – is the connection between machines reacting to each other. This enables the emergence of not so obvious connections, for example, a coupling between economics and ethics: if an ethical product is more profitable than a non-ethical one, the former is chosen. This refers to the issues that count, to which the markets react. Machines come with different values through which they seek connections to other machines, through which they subject and become subjected. What does this mean on the practical level? How do these subjective connections of the abstract machinery manifest themselves in front of our eyes?

The internal logic of the market requires that production is kept running as long as there is a demand for the product. Depending on the organization (which vary in size and strategies), protective machines may be deployed on different levels, for instance by installing a firewall. With the firewall purchased (or self-developed) and installed we have a connection, a link between profit-production (with an 'owning machine', if we blend in a combination of Luhmann's and Deleuze & Guattari's terms) and security machine that is manifested by the firewall. It is the whole thread of agents, knowledge, and usability studies that serves the starter, the igniter – value. Moving towards the business dimension, a firewall comes with costs, and every investment, including firewalls, has value that is – at least – fantasized to be measured. In fact, models have surfaced that seek the evaluation of return on information security investment (Magnusson et al. 2007, Sonnenreich et al. 2006). In other words, the success and perhaps the entire existence of information security is interpreted in terms of economic growth. Gordon and Loeb (2005) present a framework for cost-benefit analysis with the preliminary intention of addressing three aims: (1) to find out the optimal level of funding, (2) to understand how resources should be allocated among projects, and (3) to discover how Chief Information Security Officers (CISO) can develop business cases for projects. For example, the productivity paradox states that in the case of information security, the best possible outcome is that after investments nothing happens (Magnusson et al. 2007).

As IT budgets rise, the focus is changing from saving costs to contributing to the business. While the frequency and cost of security breaches has increased, the importance of economics has become a central issue (Cavusoglu et al. 2004). In fact, several authors suggest cost-benefit analysis to help in investment decision making regarding information security (Gordon & Loeb 2006, Mercuri 2003, Bojanc & Jerman-Blazic 2008). This is to underline the relation between value and information security: the one is to serve the other, and the value (growth) aspect has risen as one dominating line of thought. Briefly, value considerations are the central feature of the business world. To put it simply, an organization seeks to maximize value creation in order to add shareholder value. In practice this means that an organization attempts to decrease functions that do not create any value

and increase activities that produce a desirable result (Magnusson et al. 2007). Thus, information security that does not increase value is a waste of resources in this view. Information security has no function in itself; it has to have valuable assets under its protection, from which the reason for the existence of information security derives. Information security is a machine assembled to the value-producing – usually proprietary-based – machinery that is connected to the markets and the world of business.

Alongside this view, Magnusson et al. (2007) argue that, following the principle of value creation, 'Net Present Value (NPV) calculations for IT security investments should be drawn up to "compete" with other investments on the same conditions and to be a part of the value creation.' Thus, we argue that value (tangible and intangible) precedes information security by fuelling the machine or acting as a launch pad. Therefore, information security as a field is like a medusa that is being twisted in different directions, for example, it should enable and support the goal and ultimate function of the organization. Just as information systems themselves should not be the target or goal of work, but tools that enhance the work itself, information security does not exist in a vacuum; it supports, upholds and protects the functions and processes of the organization in order to attain the vision of the organization. However, value creation has an internal and immediate, as well as external and long-term goals, which puts the machine into a schizophrenic state: (1) the information security department should compete with other departments, while facing the productivity paradox (the best case scenario is that nothing happens), and (2) it should, at the same time, support the grand strategy, meaning that it must support other departments, and focus on the outcome of the organization as a whole. If it cannot compete with other departments, its funding is reduced, thus it cannot perform its function, supporting the overall strategy. By making it compete with other departments, it is no longer an integral part of all functions; it is being made to stand on its own. Another example illustrates this schizophrenic state even more clearly: if a company sells software applications, should the sales team compete with other departments with bonuses as the reward? The making of the product includes other departments: the logistics and other functions that have an impact on customer satisfaction, all supporting functions that enable the sales team to reach their goal, also play a part in the sales outcome. In fact, it would be logical for other departments not to help the sales department in order to shine brighter in comparison, and receive greater rewards. This example also illustrates the fact that other machines and sources of value exist outside the security machine.

But as we have claimed, value may have multiple sources; value may be driven into the security machine from multiple points. It is not just economic value that starts the machine. Privacy, for instance, is valued and may initiate the security machine as well. Internet users can value privacy, the insurance that personal information on their behavior regarding browsing and shopping is indeed personal and private. There are other examples of privacy as well, such as medical records. If information about who has sexually transmitted diseases or diseases such as HIV was public, it could easily lead to discrimination. These situations summon security machines as well. Furthermore, we would like to stress the fact that value and the security machine have a strong relation. However, it is not a universal rule that they always correlate: a code wizard may initiate a security machine (a firewall for instance) solely to try it out, without a direct connection to value. In any case, this signifies that the security machine does not stand alone but is connected to various machines that feed power into the machine. In addition, we have claimed that value has numerous references. First it is something that is appreciated in the system (functional value), which makes the protection of the object desirable. In the economic system, value plays a dual role: it is profit that is valued, that constitutes rationality in the system. Thus objects are appreciated if they can be utilized as a means to profit. As the rationality is 'to profit as much and efficiently as possible', any object that comes in the way of the 'economy machine' is treated with this rationality. Therefore the security machine is also subjected to this rationality, which makes it fair to say that the security machine is – in the business world at least – the servant of value rationalities.

4 TERRITORY

Information – defined as data – always lies in the physical space and carries a precise order that may be constructed on series of numbers, letters, or can be a picture, a blueprint, etc. Since information necessitates a piece of the physical space, there is a territorial aspect embedded within 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, e.g. signs, digits or diagrams. Information stored in memory devices is of course familiar to computer users, but it should not be forgotten that information media can be found in the human body as well: cells carry information coded within DNA (cf. May 2006, 48). So there is always a medium, without which information cannot exist. Again, information occupies a material space, a medium.

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, again, of its counterpart, the *virtual*. There is virtual information that can be derived from actual information, deciphered from perceptions, reduced, logically argued, etc. Actual information is something that is "here" and present, while the virtual includes information that can be brought in the domain of the actual. A distant memory is virtual if it is not thought of, but as it is recalled the memory becomes actual. (See May 2006, 45–52.) This means that we can have information that is not actual information but which has the possibility to enter the material world.[2] Alongside the aspects of virtuality and actuality, time begins to play a role: information in terms 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, 45–52; cf. Foucault 2003a, 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 – perhaps the most important property of information – to consider: the order of the information. With this 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. Information is not chaotic but directional (cf. Deleuze & Guattari 2004b, 344–345). It is organized within the material appearance, which refers to its territoriality.

'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) and, then again, there are territories that are established to protect information. The security machine has to establish or deploy its activity into a space that it starts to shield. It is firstly *the order of information* and secondly *the space that the information occupies* that are protected. These *safe zones* are, nevertheless, surrounded by uncertainty, the forces of chaos outside. The phrase 'forces of chaos' may sound like a dramatic and mystical term (almost science fiction!), but it actually refers to the more banal movement of different particles. This chaotic movement is the beginning of everything, including order and organization. Grosz writes, in a Deleuzian manner, of how chaos gives birth to the fragile order that is life, a term that could be easily replaced with 'a piece of information', which holds another order:

> In the beginning is chaos, the whirling, unpredictable movement of forces, vibratory oscillations that constitute the universe. Somewhere in this universe, in a relatively rare occurrence, this chaos, through chance, generates organic proteins, cells, proto-life. Such life can only exist and perpetuate itself to the extent that it can extract from the whirling chaos that is nature, materiality and force, those elements, substances, processes that it requires, that it can somehow bracket out or cast into shadow that profusion of forces that engulf and

[2] The case of the development of the security machine, which we have already mentioned, is similar: there is also the virtual side of the security machine, the state of becoming, in Deleuzian terms.

> surround it so that it can incorporate what it needs. And such life can only evolve, become more, develop and elaborate itself to the extent that there is something fundamentally unstable about both its milieu and its organic constitution. (Grosz 2005, 16.)

Therefore, in terms of information security, the order born from chaos – the piece of information – is in a fragile state, in danger of slipping back into chaos. An example should make the discussion more concrete. A hard disk, assembled in a production line, constructed of pieces of material, configured precisely, constitutes a functioning storage medium. Solid stability of performance is sought, but unfortunate breakdowns do occur, and accidents, for example dropping a laptop, do happen. The physical failure of a hard disk caused by an outside force poses a threat in terms of information security, since it scrambles the order on the disk and, in the worst case, makes the data irretrievable. It is the organization of information that is lost. There are safety measures such as free fall detection systems inside laptops or SMART (Self-Monitoring, Analysis, and Reporting Technology) applied to the majority of new hard drives. These measures 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 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 restoring back-ups 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, threatening 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 (Deleuze & Guattari 2004b, 343–347). It is this line or frame that creates a territory out of chaos (Grosz 2005, 19). It is important to note that 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. The security machine is 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' – in the animal world these might be droppings, for instance (see Deleuze & Guattari 2004b, 348–250). In the case of companies, a logo or name on the building announces a border, the beginning of the territory. Placards can emerge in a more subtle way, such as in the form of a closed door, or in any other kind of reference to an entrance, such as a doorbell or a door phone: a sign of an access point. In terms of information security, standards such as ISO 17799 describe the function of physical security as setting barriers in order to hinder outsiders from getting in (Bosworth & Kabay 2002). 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 means that the division between the inside and the outside is standard. This division establishes a categorical difference between us and them, insiders and outsiders. Borders do not emerge merely on the physical level, either. Technical walls are also erected: a firewall is the most obvious of these kinds of walls. A firewall follows the most basic digital pattern: – in Shakespearian terms, to be or not to be – 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 announcing the borderline between inside and outside. A pop-up window that requests a user name and password is another border-placard.

The social level includes walls as well. Compliance deals and rules of conduct regulating how to handle information erect walls that seek to keep information inside. Policies pursue the same goal. Information can be labeled according to various categories, such as confidential, secret, and top secret. Defining certain information as belonging to a certain category determines social-level regulations as to how the information should be treated, who can access it, where it may be accessed, how it should be encrypted, how it is to be stored and erased, and so on. 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, 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 within the reach of the security machine. For example, he or she might have agreed to a non-disclosure agreement, promising that the information in their brain will not be revealed to other outsiders. This security machine seeks to ensure that the information stays inside.

At this point we have to remember the dual role of territory: there are the valuable assets that carry inner order (e.g. a file on a disk) and then there is the other territory – the safe zone – that possesses 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 hierarchal one: the one serves 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. 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 is the door and the lock, but if we are approaching the issue of information security, it seems as though the order is CIA/IAA, which is harnessed to keep the valuable assets safe. 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 very 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 the practical level, 'confidentiality' pertains to secrecy, meaning that not everyone can reach the information, but only certain selected agents. This indicates that the physical space reserved by the information is confined, walled in. For instance, 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 first type of territory – the territorial side of information. 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 are not arguing that if IAA is carried out then the aim of CIA is necessarily reached. IAA is simply a proposal that many security machines have captured and connected to themselves. Furthermore, it should also be noted that plenty of measures have been developed which 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, 345) claim that a rhythm is an answer to chaos. Insiders at every level are made to function to this rhythm. To become an insider is to begin to resonate with this rhythm. However, the complexity of the situation is apparent, since IAA is just one rhythm of the inside. Compliance deals are not IAA, but control of the inside, to keep information inside through social regulations. IAA is an important technical rhythm that leads to the idea of user accounts, making divisions within the territory. IAA organizes the inside. For instance, every user account has its own space that consists of 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. Users are not equal but are usually divided into hierarchal categories: for example, a Chief Information Security Officer typically has more administrative privileges than an average employee.

All in all, territories deal with insides and outsides, and can be placed inside each other to give territories within territories. Furthermore the situation is dynamic as territories constantly move in relation to each other. Attempts are made to keep the inside in controlled order, but there is constant movement within inside territories. A file can be copied, modified, and transferred. Territories are not quiet, they are filled with teeming movement. Still there is a desire for hygiene on different levels: a virus scanner is responsible for keeping its territory clean (see Parikka 2007), a door code seeks to keep outsiders outside, etc. Because the outside elements threaten the territory, it is placed under

constant maintenance. For instance, walls and fences are fixed if they are broken down, and firewalls are updated, as are virus databases. Again, it is a question of the order of the inside.

5 CONTROL – SUBJECTIVATION

The next question to arise is that of how insiders become insiders. The question may seem misplaced since we already know the answer, which is provided by IAA: users are identified, authenticated, and authorized as insiders. But IAA is just the first step; indeed at this point users are insiders, but what this means is to be subjected by all the levels of territory[3]. As the territories are established to protect valuable assets (and the production of valuable assets), they aim to have a controlled inside. The agents on the inside, whether human or non-human, are components of the ordered territory, but they also simultaneously pose a potential threat to the order; agents may appear not to be as reliable as desired. A user who does not pay attention to the rules for creating proper passwords but simply picks a word from a dictionary eases the job of brute force cracker. A similar problem emerges if users do not change their passwords frequently enough. Obviously, these problems are quite easily dealt with using a straightforward solution: the system is provided with an application that automatically checks for weak passwords and forces users to change their passwords on a regular basis. The important point here is not the triviality of these problems, as they are easily dealt with, but the direction from which a way out of the problem is sought – namely, from technical solutions. It seems that users are a necessary problem; they cannot be controlled entirely, so control is sought using technical solutions. Moreover, problems arise not just as a consequence of unpredictable behavior (e.g. password problems), but due to the whole situation in which humans are present as users. Therefore, techniques for detecting when a speaker is lying in a phone conversation, through technical audio analysis, have been developed (Hollien et al. 1987). In these techniques, an automatic technical solution, rather than a human agent, flags a warning. It is not important whether the lie-detection technique works or not. Instead, it is the direction that matters: there is a clear desire to let the technical machinery take care of as many issues as possible. A good example is another solution, under enthusiastic development, to the password problem mentioned above. As well as by using passwords (identification by what the user knows), legitimate users can be identified by referring to who they are, for example using biometrics or behaviometrics (see Nisenson et al. 2003). Users can also be identified according to what they have, for example tokens that do not require any human element in the process. With solutions that are based on a user's 'essence', password changes do not play such an important role, since there is another line of defense behind the password inquiry. In other words, password quality is no longer such a critical problem, if passwords are not the only measure in IAA. The crucial point lies here: in both of the solutions, the security machine reaches for another technical component of control with which it seeks to sustain the order of the territory. In other words, solutions to the problem of identification have emerged, as part of IAA, that are critical (at least for now) for the security machine. Again, the security machine is open to change and is ready to devour new ideas.

So we have a triumph of the technical level, but what does it really have to do with becoming an insider? The insider question is about subjectivation. Territories are about creating and sustaining order through IAA (to protect the CIA of information), and as the technological level changes, it subjects users to the changes. The machine molds its users; not completely, but it creates action. As mentioned in the 'Machine' section of this paper, to place a door somewhere is to subject its users to it, to its location, and to its function. In the same way, we can continue the example of passwords expiring, since if the password is not changed when the system requires, the user simply cannot log in, as the password is defined as invalid by the system. The security machine makes users act, and it does so on three levels. But users are not coded, because they cannot be programmed as a technical device can be. The security machine tempts people to behave in a certain way, by using positive power,

[3] The term 'subjectivation' refers to the birth of the subject – in other words, how one makes oneself a subject in relation to something. This subjectivation always requires subjection. In the case of the security machine, the machine provides activity and territory to which one is subjected. We hold that being subjected by the security machine leads to subjectivation, since users have to think of themselves as users. This requires a relation to the self. (See Foucault 199, 26–32.)

educating, guiding, and paying salary (cf. Foucault 1998, 136). Therefore, to be an insider is to be subjected to the territory. This means that users, as insiders, are subjected to best practices, which *positively* offer knowledge on how to behave well from the viewpoint of information security. In other words, knowledge is offered on how to serve information security that has inherited the ideas of the economic system, and how to behave in such a way that ensures the safekeeping of the secrets, the valuable objects. This is, in other words, an education in how to be a good insider. From the viewpoint of information security, anyone with an authenticated identity is a chosen one. They play along to the tune, or the rhythm, of the territory. The chosen ones are consistent with the rhythm, since they are system-generated. However, being a chosen one means no more than holding a user account with some privileges, and becoming subjected.

With the aspect of subjectivation, we seek to emphasize the initiator role held by value, which is behind the security machine (see the 'Value' section of this paper). It is value generation that summons the machine and summons the subjection as well. Value constitutes rationality that legitimizes action and provides meaning for the techniques that are applied. Protection, whether it emerges in the form of buildings, architectural solutions, or digital information systems – all of which subject users – serves the valuable assets. Everything is placed, through various techniques, under control, which generates the rhythm. Moreover, we really do mean 'everything', not merely 'users'. Technical agents (e.g. firewalls) are subjected as well. As we mentioned in the 'Machine' section, to configure a firewall is to subject it. Some parts of the entire system are easier to control, such as digital solutions: a program's code can be altered. The human element poses a greater challenge for the system, as is very well-established throughout the field of information security (see Stanton & Stam 2006, Tipton & Krause 2004, Bosworth & Kabay 2002, Mitnick et al. 2002, Winkler 2005, Long et al. 2008, Schneier 2004).

6 THE FIREWALL THOUGHT AND PENETRATING CHAOS

In this section, we would like to show some dysfunctions of IAA/CIA territories and security machines, and also locate these failures. The first problem emerges when we combine subjectivation of users to the division thought and the triumph of technical agents. As we already know, territories are all about creating an inside order against the outside chaos, and it is IAA that tries to provide an order. IAA aims – as has been mentioned – to protect valuable assets, and the same is true of the walls which are erected by the machine. IAA then produces – through various techniques – a distinction between hostile and friendly. This is a division between chaos and order, among the inhabitants of the system. It does not make a great difference whether the inhabitant is machine or human, since they are both subjected to the system. They vibrate the rhythm of the territory – an order separated from the outside chaos (Deleuze & Guattari 2004b, 345). This divisional practice functions on distinctions: accepted/rejected, authenticated/not authenticated, and insider/outsider. As we have seen, protection – as well as subjection – takes place at several levels: the technical, the physical, and the social (including the educational). At every level, control is sought. However, rather than being separate, these levels are folded in on each other. Therefore, a change at the technical or physical level will have an effect at the user level, as this is a subject of the territory. The firewall thought – which is simply a belief in the division between allowance/rejection as a result of IAA – molds the social reality; it subjects the agents in its regime. As seen in the previous section, there is a desire to place responsibility for protection on the technical and physical levels, leading to the triumph of technical measures. However, the pervasive force of the technical level may carry a dysfunctional element as well. As the ideal is to make everything the responsibility of machines, and the technical level (along with the concrete level) constantly carries out a huge proportion of security tasks, trust is built up among users. The notion of IAA is there to secure the emergence of an inner circle – a territory that is filled with insiders, individuals who belong there, who have a purpose (a task or a position) there. This is to say that, within a safe zone, the user is surrounded by friendly insiders. As a user or employee, we believe that everyone who is with us, who has gone through several IAA checks to get inside, really is an insider. According to the firewall thought, if they were not insiders they would have been rejected. However, what if an outsider was to take on a false identity? A skillfully camouflaged agent, for example a social engineer, who manages to gain the identity of an insider is

free to mix with other insiders without being questioned. The trust in the security makes the system blind to normality. It makes the normal invisible[4]; this means that the insiders – the inhabitants of the territory – are invisible as well. If a social engineer adapts to the rhythm of the territory, an opportunity for him or her to change from a visible outsider into an invisible, normal insider surfaces. A jump into the net of insiders through compromised IAA provides validity through false authentication. It brings cover and silence. Mitnick et al. (2002) provide several examples of an intruder infiltrating a territory posing as an employee, creating the appearance of normality, and stealing information once his or her position is established (as a legitimate insider). Subjection of the firewall thought – where the idea of the protected inside is imprinted on everything – can produce opportunities for penetration among social agents.

Furthermore, the firewall thought does not look inside the territory, since its task is to keep up the division, to manage the tunnels, guaranteeing authorized access. Nonetheless, there are systems (within territories) that do take a look inside, such as intrusion detection systems (IDS). The precise function of these systems is to search for abnormalities that are visible: an IDS raises a flag in case of abnormality. However, the gaze – a surveillance camera for instance – records the story of the inside as well as of the borders of the territory. Because of this, suspicion arises, as the system watches the inside as well. This is a discipline machine (cf. Foucault 1991).

The question of normality does not stop here. In the case of rootkits, malicious code hides itself under core processes, which make rootkits invisible from the surface. To become invisible is to become normal. The security machine is open to changes and reacts to environmental transformations. Just as there is an intrusion detection system on the firewall side, technologies have also been developed that seek to unveil secrets on the rootkit (virus-scanner) side. These include methods (whose names even refer to shedding light in the dark) such as the BlackLight technology introduced by F-Secure.[5] BlackLight is a response to change, and it would not have emerged had rootkits not existed. This reveals the picture of the security machinery in which the machines are connected to each other, producing desires (value thinking), producing security (order), producing lines of flights, objects that escape the security machine creating something new, e.g. rootkits, social engineering, and different methods of identification (see Deleuze & Guattari 2004a, 2004b, 4).

The secret at the center is the object that has to be accessed by some (authorized individuals only), denied to others (with IAA implemented throughout to carry out this task), with the machinery directing other machines on their respective jobs. It makes no difference whether the machine is a human, a firewall, or a camera. They all are connected to other machines, serving their own rationalities which are constantly on the move in the flux of rationalities. The first layer of rationality that initiates the security machine is motivated by the value thought: 'valuable assets have to be protected'. The summoned security machine then starts the creation of territory; walls are erected. At this layer the rationality is motivated by protective action: any activity that contributes to the task of protection is considered to be rational. But as the territory has to meet the requirement of availability (CI*A*), a controlled filtering system between inside and outside becomes rational as well. These rationalities are not merely rationalities of the inside, because if a social engineering machine from outside tries to capture information from inside, the situation turns into a struggle between machines from outside and inside.

However, both still share a desire for the object; they both acknowledge its value. A situation with one machine trying to keep the secret (the security machine) and the other machine acting as a chameleon (a social engineer penetrating a territory, taking on the position of an insider) creates a tension around the secret that is desired. The one machine tries to keep the secret, while the other yearns to discover it. The desire for the object is shared, but something else is producing the desire here. There are two machineries around the secret; nonetheless they serve the economic system (value) or a prestige system (a cracker proving to him/herself that it is possible to break in). In any case, there are power

[4] Normality is invisible in sense of imperceptibleness. It is abnormality that draws attention and tends to be corrected (see Foucault 1991, 177-184; 1998, 105).
[5] See http://www.f-secure.com/blacklight/

relations involved. Two machineries test their strength in the flux of desires. The territory lies in between the two.

It is rather pointless to list everything that could go wrong. Instead it is interesting to see *how* things go wrong. All the failures seem to pertain to distorted order as something from the outside penetrates the inside, shattering the organization. It is the forces of chaos which tear down order. However, there arises an important question: where is the penetration of forces if territory is a closed circle? Firstly, it is not in fact a closed circle – total blockage – since there is the requirement of availability (CI*A*). As information is made available through different filtering systems (e.g. an IAA-based SSH tunnel), territory opens up and stretches its tentacles outside. A distant user enters into discussion with the territory through the chaos. Obviously, the connection – the discussion – is encrypted; in other words, it is camouflaged as chaos. Every blocking level opens up possibilities for penetration. However, this is still not the crucial point. If we look carefully at how a territory is created, the answer to the distortion of order becomes clear: everything inside the territory is brought in from the chaotic outside. The territories are made out of chaos; they are just organized. As mentioned when discussing the maintenance of territory, for example, fixing a broken wall, everything that is needed to repair the wall has to be brought in from the outside. From the security point of view we have to understand that information systems are also territorial, and they are constructed within chaos and from the materials of chaos. We have mentioned a hard disk: consider the materials from which it is made, and where the molecules making up the components of the disk had been previously. The actual answers to these questions are trivial, but this example demonstrates that materials are never pure but also have elements of chaos with them. Serres (2007, 79) claims that no system is noiseless. A virus or a bug is noise within an information system (Parikka 2007). From a security point of view, outside materials are constantly present on the inside. The territory is an arbitrary attempt to enclose the inside away from the outside, but it simultaneously brings particles in from the outside.

A security patch provides another example. It comes from the outside, and it has been realized that patches can be dangerous to the system. Installing new patches has even been connected to value thinking, as there is a study on calculations of the optimal time to install a security patch. The best moment – if we do not wish to crash the system – is not immediately after the patch is released, because it is not yet known what undesired effects it will have on the rest of the system. (Beattie et al. 2002.) The outside is everywhere within the territory: programs, devices, cameras, people; these all originate from the outside. Inhabitants of the territory inhabit other places too. With humans comes a special problem relating to chaos. When humans are involved, we can have any number of varied ethical codes, norms, and regulations with which the security machine seeks to control human behavior. The normative aspect is very clear: people are told to behave in a particular manner (e.g. compliance deal, guides for handling sensitive data), but the code alone is not enough, it has to be actualized in action. However, in order to carry out an ethical code, individuals have to establish a relation between the self and the code; they have to subject themselves in some way to the code (Foucault 1992, 26–32). For instance, if users are told always to lock the computer when they leave their desktop, the rule is clear. However, it is not clear how seriously users will take the rule. There are different ways to subject oneself to the rule. One user may do nothing except try not to forget the rule, another may write a note and place it next to their computer, while a third may even read the security guidelines every night, in an attempt to become a better user. This relation to the self is another outside fact which may disturb the inner order. As with everything that is brought in, humans carry extra weight as well. Metaphorically, there is some dirt on their shoes which has to be taken care of by the cleaners (cleaning is partly creating the order). Employees may not spend all their time at work thinking about work-related issues. Once again, there is no clean inside, as everything inside a territory is brought from outside and made out of the materials of chaos, and, furthermore, as the security machine is ready to absorb anything from anywhere if it fits its goal of protecting valuable assets. Thus, the question we need to ask about the collapse of order is whether we should talk in terms of the penetration of disorder, or the importation of chaos.

7 CONCLUSION

While CIA remains the classic definition of information security, which is served by IAA, we introduced the security machine in order to reveal the complexity of information security. Instead of focusing on individual security patterns and safeguards (a collection of do's and don'ts), a fresh perspective was sought, at a higher level of abstraction. For this purpose, a new way of looking at information security was required. Rather than describing existing security patterns, we wanted to explore more fundamental questions, such as: why does information security exist? What is it exactly that it does? How does information security function in different environments?

To think about security as a machine is to describe it as a dynamic environment, where nothing stays fixed. The machine itself is open to change; it is in a state of becoming and can take one of an infinite number of routes. It absorbs new ways of thinking from the fields of science, which cannot be controlled by anyone. No one knows what science will come up with in the future. The machine is open to change in another manner as well, in that it grabs new equipment as it is developed. On the other hand, the machine also fails in its connections. Some of the components it reaches for may be found to be non-functional, and the machine may disconnect itself. For instance, weak encryption is abandoned as the processing power of computers increases. Constant value thinking feeds the security machine, in other words the rationality of value thinking devours the machine. The security machine serves value by protecting valuable assets, but at the same time the machine itself is considered in terms of value, and how expensive the machine is, in relation to the goals that it achieves. Moreover, in the case of security, we cannot know whether the goals have been achieved without using some form of measuring mechanism, an area to which a number of scientific studies have been devoted. Territories are established in order to protect valuable assets. Spatial and temporal issues, an integral part and central trait of the security machine, become visible as information does in fact require physical space. Besides space, there is the requirement of inner order of information, and additionally, there is always time for information to surface. The question becomes, then, one of defending these physical sites and the order (integrity) of information. Information is territorial as it reserves a space and time. The territory of the information has to adhere to the rhythm of CIA: information is confidential and has to stay in order instead of being corrupted or illegally changed (integrity), but it must also be accessible to those who require it and are authorized to access it (availability). The answer to the question of CIA at the moment seems to be the creation of a safe zone (another territory) around the object that is to be protected. The surrounding territory has another order, which is IAA. As long as IAA is not compromised, the initial informational territory stays intact. The problem is that of how to wall the territory but still let people in and out of it – in other words, how to maintain the order of the territory that protects the information territory.

Protective activity takes place on several levels that all try to erect walls between the ordered inside and the chaotic outside that is constantly trying to penetrate the inside order. There are walls, fences and doors that connect to each other forming a physical layer. There is technical equipment (firewalls, IDS, virus scanners, etc.) implemented in the physical environment. Socially, territory is controlled by demands on behavior. The most difficult component in the machine is the human. They are necessary, but the human element is affected by the desire for it to be controlled in the same way as other agents (such as doors, walls, and firewalls). Thus, users and employees become subjected to security patterns on three levels of the machine. The employee is subjected to compliance deals (social), certain physical movements are allowed or restricted as well as monitored (physical), and the issue of access to information systems also subjects the employee (technical). We emphasize the triumph of the technical level, which through IAA subjects users to the need to change their passwords at a given interval (depending on the policy), forces them to pick certain type of passwords, and so on. With the goal of keeping the order inside, and the insiders as legitimate insiders, subjectivation refers to the subjection by the security machine of the agents on these levels. The security machine produces a certain kind of users – at least, it seeks to control the users.

As everything is based on the notion of territories, the firewall thought is created. This is a division between insiders and outsiders. But there is no way of creating total blockage: territories need things from the outside. Where else do the users and employees come from, but from outside? Where else

does the technical equipment come from, but from outside? The territory is in constant contact with what is outside. The territory is an arbitrary attempt to wall the chaos out, but everything inside initially comes from that chaos. This is the reason that the security machine is constantly on the move: it tries to fight chaos with elements that originate from chaos. The struggle to purify the elements of chaos when they are brought in to protect valuable assets (that also are brought in from outside), is revealed as the ultimate task of information security.

References

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

Bojanc, R., Jerman-Blazic, B. (2008). "An economic modelling approach to information security risk management. International Journal of Information Management", 28; 413–422.

Bosworth, S., Kabay, M.E. (2002). "Computer security handbook", John Wiley & Sons, New York.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). "A model for evaluating IT security investments", Communications of the ACM. 47(7); 87–92.

Deleuze, Gilles (2006). "Foucault", Continuum, London.

Deleuze, Gilles and Guattari, Félix (2004a). "Anti-Oedipus: capitalism and schizophrenia", Continuum, London.

Deleuze, Gilles and Guattari, Félix (2004b). "A thousand plateaus: capitalism and schizophrenia", Continuum, London.

Foucault, Michel (1990). "The care of the self. The history of sexuality volume 3", Penguin Books, London.

Foucault, Michel (1991). "Discipline and punish: the birth of the prison", Penguin Books, London.

Foucault, Michel (1992). "The use of pleasure. The history of sexuality volume 2", Penguin Books, London.

Foucault, Michel (1998). "The will to knowledge. The history of sexuality volume 1", Penguin Books, London.

Foucault, Michel (2003a). "The Archaeology of knowledge", Routledge, London & New York.

Foucault, Michel (2003b). "The order of things", Routledge, London & New York.

Foucault, Michel (2004). "Madness and civilization", Routledge, London & New York.

Gordon, L.A., Loeb, M.P. (2005). "Managing cybersecurity resources: a cost-benefit analysis", McGraw-Hill, USA.

Grosz, Elizabeth (2005). "Chaos, Territory, Art. Deleuze and the Framing of the Earth". *Idea*, 15–28. Also available at <http://www.idea-edu.com/Journal/2005/2005-IDEA-Journal>.

Hollien, H., Geison, L., Hicks, Jw Jr. (1987). "Voice stress evaluators and lie detection", Journal of Forensic Sciences. 32(2); 405–418.

Latour, B. (1992). "Where are the missing masses, sociology of a few mundane artifacts." In Bijker, W., Law, J. (eds) *Shaping technology-building society: studies in sociotechnical change*, MIT Press, Cambridge Mass.

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

Luhmann, Niklas.(1989). "Ecological communication", University of Chicago press, Chicago.

Magnusson, C., Molvidsson, J., Zetterqvist, S. (2007). “Value creation and return on security investment (ROSI)”, In IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, (eds) Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. Boston, Springer: 22–35.

May, Todd (2006). “Gilles Deleuze: an introduction”, Cambridge University Press, New York.

Mercuri, R.T. (2003). “Analyzing security costs”, Communications of the ACM. 46(6); 15–18.

Mitnick, K.D., Simon, D., Wozniak, S. (2002). “The art of deception: controlling the human element of security”, John Wiley & Sons, Indianapolis.

Nisenson, M., Yariv, I., El-Yaniv, R., Meir, R. (2003). “Towards behaviometric security systems: learning to identify a typist”, Knowledge discovery in databases: PKDD 2003. Springer, Berlin.

Parikka, Jussi (2007). “Digital contagions: A media archaeology of computer worms and viruses”, Turku.

Schneier, B. (2004). “Secrets and lies: digital security in a networked world”, John Wiley & Sons, New York.

Serres, Michel (2007). “The Parasite”, University of Minnesota Press, Minneapolis.

Sonnenreich, W., Albanese, J., Stout, B. (2006). “Return On Security Investment (ROSI) – A Practical Quantitative Model”, Journal of Research and Practice in Information Technology. 38(1); 45–56.

Stanton, J., Stam, K.R. (2006). “The visible employee. Using workplace monitoring and surveillance to protect information assets – without compromising employee privacy or trust”, Information Today, Inc, New Jersey.

Tipton, H.F., Krause, M. (2004). “Information security management handbook”, Auerbach Publications, Boca Raton, USA.

Winkler, I. (2005). “Spies among us. How to stop spies, terrorists, hackers, and criminals you don’t even know you encounter every day”, Wiley Publishing, Indianapolis.