De-perimeterisation as a cycle:

tearing down and rebuilding security perimeters

André van Cleeff, Roel Wieringa *

December 5, 2008

Abstract

If an organisation wants to secure its IT assets, where should the security mechanisms be placed? The traditional view is the hard-shell model, where an organisation secures all its assets using a fixed security border: what is inside the security perimeter is more or less trusted, what is outside is not. Due to changes in technologies, business processes and their legal environments this approach is not adequate anymore. This paper examines this process, which was coined de-perimeterisation by the Jericho Forum. In this paper we analyse and define the concepts of perimeter and de-perimeterisation, and show that there is a long term trend in which de-perimeterisation is iteratively accelerated and decelerated. In times of accelerated de-perimeterisation, technical and organisational changes take place by which connectivity between organisations and their environment scales up significantly. In times of deceleration, technical and organisational security measures are taken to decrease the security risks that come with de-perimeterisation, a movement that we call re-perimeterisation. We identify the technical and organisational mechanisms that facilitate de-perimeterisation and re-perimeterisation, and discuss the forces that cause organisations to alternate between these two movements.

*Information Systems Group, University of Twente, The Netherlands. http://is.ewi.utwente.nl
Contents

1 Introduction 3

2 The concept of de-perimeterisation 4
   2.1 The Jericho Forum .......................... 4
   2.2 De-perimeterisation phenomena .............. 5
   2.3 Perimeter structure .......................... 7
   2.4 Definitions ................................. 8

3 De-perimeterisation mechanisms 9
   3.1 Scaling up: From private to public space ........ 10
   3.2 The firewall: Separating private from public ....... 10
   3.3 Technological de-perimeterisation mechanisms .... 10
   3.4 Organisational de-perimeterisation mechanisms .. 12

4 The dynamics of the re-perimeterisation cycle 14
   4.1 Security impact .............................. 14
   4.2 The re-perimeterisation cycle ................. 16

5 Re-perimeterisation mechanisms 17
   5.1 Technical re-perimeterisation .................. 18
   5.2 Organisational re-perimeterisation ............. 22

6 Discussion and further work 26
1 Introduction

All need for security starts with the fact that there is an asset that is potentially threatened by an “outside” influence. It needs to be protected. Because of this need, we define the policies that should be used to secure it and implement the necessary technical measures. However, such an approach is only possible if we can identify the asset, why we want to protect it and actually have the capabilities to do so. In a networked world, this is often not the case. We don’t know what or where the asset is, we are not sure about its value and we have no way of securing it through our own intervention. For example when we outsource, or when we rely on services of others, we are faced with the question: how should we deal with security when assets are so ill-defined and intangible?

This is an important question today, and we can expect that it will be even more important in the foreseeable future. Already we are seeing devices and applications that further blur the IT security landscape. Mobile devices can access data from anywhere, smart buildings are being equipped with small microchips that constantly communicate with each other (and their headquarters). With so-called cloud computing, organisations can rent virtual PCs by the hour [36, p.23]. This leads to even more complicated systems, or systems of systems, which span the boundaries of multiple parties and cross the security perimeters that these parties have put in place for themselves. Following the Jericho Forum [14], we call this process de-perimeterisation and it will be the focus of this paper.

Obviously, security can be improved by many types of controls, ranging from screening new employees to physical access controls in data centers (Cf. Kartseva [20]). Here, we are mainly concerned with IT and organisational mechanisms. We will investigate two kinds of mechanisms that foster security in the presence of de-perimeterisation

- technical mechanisms inside of IT; meaning (parts) of applications, specific IT architectures that can improve security.
- organisational mechanisms; meanings structural changes in the way organisations cooperate

Our approach is as follows: First we identify and analyse in section 2 the phenomena of de-perimeterisation and the structure of an organisation’s perimeter that makes these phenomena possible. This leads to definitions of the concepts of perimeter and de-perimeterisation.

Next, we identify in section 3 the technical and organisational mechanisms that in the past decades have led to de-perimeterisation on an unprecedented scale. In section 4 we show that the dynamics of de-perimeterisation is cyclical. De-perimeterisation is basically an increase of connectivity. However, the pace of the increase is not fixed. At times it accelerates, followed by a period of decelerated increase that we call re-perimeterisation. De-perimeterisation is driven by a desire for increased speed and flexibility of business and a reduction of the cost of doing business; re-perimeterisation is driven by the need for accountability and for a proper allocation of benefits. In the balance, the trend is towards increased connectivity but the dynamics of forces towards increase and forces towards decrease leads to an oscillation. We analyse this in section 4.

In section 5 we then review the technical and organisational mechanisms of re-perimeterisation. The contributions of this paper, as discussed in section 6, are the identification and analysis of a long term oscillation between de-perimeterisation and re-perimeterisation, and the identifica-
tion of forces and mechanisms in this long-term trend. We also discuss possible applications of these findings and we indicate some topics for further research.

2 The concept of de-perimeterisation

2.1 The Jericho Forum

In order to analyse the problem of de-perimeterisation, we will first attempt to come up with a definition. What exactly is de-perimeterisation?

Since the Jericho Forum coined the term first, we will start by discussing their views. In their articles and white papers, they give several definitions of de-perimeterisation.

- *The erosion of the network perimeter.* [19]
- *The Jericho Forum coined the term "de-perimeterisation" to emphasise the trend away from the conventional thinking that focuses on security at the network boundary - security that is "hard on the outside and soft on the inside". De-perimeterisation is the trend that is happening, is inevitable, and we need solutions that respond effectively to it.* [9]
- *De-perimeterisation is essentially about redesigning the security perimeters at the boundaries between an organisation's own ICT infrastructure/services and the open networks, individuals and other organisations with which it connects.* [14, p.1]
- *De-perimeterisation occurs when two common assumptions do not hold* [14, p3]
  - an organisation owns, controls and is accountable for the ICT infrastructure it employs
  - all individuals sit within organisations (meaning: are employed by exactly one organisation).
- *de-perimeterisation is not*
  - Simply removing your border security
  - Removing / replacing your firewalls
  - Just distributing your security devices inside
  - A crusade against deep packet inspection
  - Web Services
  - Document repositories
  - A distributed data model
  - The elimination of IDS / IPS
  - A sales opportunity

*but it may involve all or some of the above.* [32, p.9]

We have found no preciser definitions in the published documentation of the Jericho Forum [9, 19, 15, 17, 16, 14].

Intuitively, the concept of de-perimeterisation is easy to understand; it is about blurring boundaries between organisations, caused by increased collaboration between businesses and individuals and the implications for IT security.

To come up with a definition, we will look at de-perimeterisation (and security perimeters in general) from two different perspectives, which each illuminate different aspects.
• The phenomenon perspective. We examine how entities “outside” a system can influence entities “inside”.
• The structural perspective: Here, we take a look at the construct “security perimeter” and its environment.

Finally, we summarise and integrate these definitions.

2.2 De-perimeterisation phenomena

De-perimeterisation is the phenomenon where increasingly, entities can influence assets of another organisation. For now we will follow the Jericho Forum by assuming that de-perimeterisation occurs when an organisation does not own or control its ICT infrastructure or is not accountable for it, or when individuals are employed by more than one organisation. We will call these the “de-perimeterisation assumptions”. To analyse what these mean, we give a number of scenarios in which these assumptions do not hold.

Some of the following scenarios are well-known, others are specific examples taken from recent news items. Combined, we have the following scenarios.

• Microsoft administers a user’s PC with automatic updates.
• Employees use laptop for private and work purposes.
• Laptops with sensitive data move physically between organisations.
• Businesses share the same virtual server.
• An ASP provides another company with an application.
• Employees access company information from outside the building.
• Different organisations hire the same individuals as personnel.
• Organisations rely on other’s IT services.
• An organisation allows remote access from another company for maintenance.
• An employee connects from home to a server of an organisation he works for.
• An employee connects from home to a server of an organisation, with which his employer has a maintenance contract.
• An employee visits the office of a prospect, with data of other organisations on his laptop.
• A social network site accesses data on another site using AJAX.
• A site uses authentication mechanisms/tokens from another site.
• An employee sends company related data from his home PC to work.
• A user visits a site of another company that has an SSL certificate.
• An organisation allows another organisation to have a look in its ERP system.
• E-bay blocks insecure browsers, thus influencing what the user can do with the browser on the laptop.
• A user stores personal information in Google Docs, with a physically and organisationally unknown location to the user.

When looking at these scenarios several recurring phenomena can be identified.
Shift from products to services  If we consider relations between businesses, it is clear that the shift from selling products to selling services is related to de-perimeterisation. Intuitively, after an organisation has bought a product, the producer does not have any influence over it anymore. This situation changes once the product is evolving (with new features or patches installed remotely) or when the product is not well-defined. For example, de-perimeterisation does not occur when a business acquires a text editor, but it does happen once its starts using the on-line version of it.

Evolving services  In fact, people use systems of which the specification is not clear - and which can even change from hour to hour, for example in the case of an on-line application. This makes it difficult to investigate how they influence each other.

Complex legal relations  As the Jericho Forum pointed out, not all persons sit within organisations anymore. Actually, the situation is more complicated - we have persons being employed by multiple businesses or working independently.

The relationship between companies may not be clear to anyone at all - sometimes business cooperate according to a contract or service level agreement, but in other cases there is not necessarily such an agreement because they are basically free.¹

We can also try to define when de-perimeterisation does not occur: Intuitively, if a freelancer works for only one company at the same time, that does by itself not lead to de-perimeterisation. In general, de-perimeterisation does not occur in a clear hierarchical legal structure. If all influences are hierarchical, there are no external influences and thus no de-perimeterisation.

Mobility  A fourth recurring theme is physical mobility. At work, a laptop might be subjected to the company’s network policies, but at home, the employee manages his own. Intuitively the security situation changes, once someone works from home:

- The laptop is connected to an insecure network.
- The laptop might not be configured according to the organisation’s policies.
- Family members might have access to the laptop.
- There is no physical oversight of the laptop and the employee.

Thus, mobility contributes to a lack of control or at least increases the influences that others have on an organisation. However, we do not believe it is an essential part of de-perimeterisation: Without mobility, de-perimeterisation still occurs.

The recurring pattern in all these de-perimeterisation phenomena is this:

A legal entity \( A \) is de-perimeterised to the extent that

- the actions of another legal entity \( B \) can influence its security during the working processes of \( A \), where \( B \) is not part of \( A \)'s hierarchy.
- \( A \) has no control over these influences or does not know their extent.

¹For example, consider the online application Google Docs
This is our first approximation of a definition of de-perimeterisation. Note that a security perimeter is a technical solution that limits these influences.

Now we define de-perimeterisation as a state that is always present to a smaller or larger extent. If an individual is a member of a committee apart from being employed at a business, this business will be de-perimeterised. We do think that this view is correct. Many organisations have procedures in place that require employees to file such relations, in order to prevent potential conflicts of interests. After all, in such a case we cannot determine whether a person’s actions are determined by his role inside or outside of the organisation. This is precisely what de-perimeterisation is about. Finally, we have to consider the question whether an individual can de-perimeterised. Logically this seems to be the case - when someone owns a laptop that features automatic updates, external parties can influence it.

Figure 1 illustrates several situations. In the first situation, A is influenced by B and has no authority over B. Thus A is de-perimeterised. In the second situation, A solves this problem by placing B under its control. The last situation shows a more complex and de-perimeterised situation, where B is under control of both A and C.

2.3 Perimeter structure

We can further improve our understanding of de-perimeterisation if we consider the structure of a perimeter and its environment.

According to Merriam-Webster [24], a perimeter is the bound plane of a closed figure and security is the condition of being protected against danger or loss. For IT this is usually defined in terms of CIA (Confidentiality, Integrity, Availability). This means that if the confidentiality, integrity an availability of a resource can be maintained, it is considered to be protected against danger or loss.

Thus, a security perimeter is a boundary between an asset and the outer world, where there is a difference between the security inside the boundary and outside of it. The perimeter can bring that difference about, but it can also be just the border. In IT, a security perimeter could typically be a firewall around a system.

This allows us to view a perimeter and its context as consisting of several elements. Usually a perimeter is not closed completely, there is traffic between the inside and outside. The traffic goes through a gate. Inside the perimeter there is monitoring, periodic security checks of the assets and the traffic. Actors, meaning legal entities such as persons or organisations, interact with, or control assets. Attacks can take place that reduce the security of the inside. From a structural perspective, then, security perimeter and its context consist of five elements shown in Figure 3.

From a structural perspective, de-perimeterisation is a process rather than a state. It is a process in which

1. the number of gates increases, or they become bigger
2. assets are moved outside of the perimeter

An example of the first trend is organisations getting faster Internet connections, the second occurs when a firewall becomes less effective or is removed, or when an organisation outsources its assets. However, there is no fixed point where an organisation becomes de-perimeterised.

One of the problems of de-perimeterisation is that this monitoring becomes more difficult
Situation 1: A is deperimeterized

\[ \text{A} \quad \longleftrightarrow \quad \text{B} \]

Situation 2: A is not deperimeterized

\[ \text{A} \quad \leftrightarrow \quad \text{B} \]

Situation 3: A is deperimeterized

\[ \text{A} \quad \leftrightarrow \quad \text{B} \quad \leftrightarrow \quad \text{C} \]

**Legenda**

- \( \text{A} \rightarrow \text{B} \rightarrow \text{A} \): A has influence over B.
- \( \text{A} \leftarrow \text{B} \leftarrow \text{A} \): A has authority over B.

**Figure 1: Perimeter and environment**

### 2.4 Definitions

In the previous sections, we have investigated “de-perimeterisation” and seen that it is driven by several trends, and that organisations are always de-perimeterised to some extent.

Figure 4 summarises the two perspectives we have taken on de-perimeterisation. Combining these, we define a security perimeter as follows:

A security perimeter is a technical solution to protect assets from negative influences originating in its environment.

This combines several elements:

- A security perimeter serves to protect an asset
- The threat originates in the environment

Turning to de-perimeterisation, the structural perspective shows that de-perimeterisation is a combination of increased and unfiltered traffic through gates in the perimeter, as well as the movement of assets outside
of the perimeter. And looking at de-perimeterisation phenomena, organisations and individuals are increasingly influencing each other, while there are no clear authority relations between them. This leads us to define de-perimeterisation as follows:

- Increased, flexible and often unknown connectivity between systems owned or controlled by different legal entities.

There are three important elements in this definition:

- Different legal entities are involved.
- New connections are created between systems.
- Connections are not clearly defined.

### 3 De-perimeterisation mechanisms

How did de-perimeterisation evolve historically? Obviously, any answer to this question requires a closer examination of the Internet; After all, it is this structure that made it possible for organisations to connect on an...
unprecedented scale. We therefore look briefly at the history of the Internet and how its development affected IT security. Figure 5 summarises the de-perimeterisation mechanisms and their impact on the security perimeter.

3.1 Scaling up: From private to public space

When we think in terms of security, it is noteworthy to point out that the Internet started as a very small place. In fact, it began with just one node in 1969, when the first computer was installed that would become part of the ARPANET, the predecessor of what we now call the Internet. By the end of 1969, there were already 4 nodes [22]. At the onset, the Internet itself was a more or less trusted system. With a limited number of servers connected to it and a limited number of people that operated those servers, there was little to fear. There was also little need for and knowledge about protecting resources connected to the Internet. After 1969, the Internet continued to grow. In 1977, there were already 111 [34] nodes, in 1988 56,000. As a place, the Internet itself became less secure; more people had access. At the same time the systems that were connected to it increased in value, making them potentially attractive targets. It also became clear how weaknesses in networks and systems could be exploited. One of the earliest attacks was the so-called Internet worm that replicated itself among hosts, starting on November 2nd, 1988 [33]. This can be viewed as the end of the Internet as a more or less private and trusted space. The Internet grew to over 36 million hosts in 1998 and to over 500 million in 2008 [5]. Today, the Internet is part of the public space and people worry about its insecurity, just like they would if it were a street corner. It is no longer the sole domain of US universities and government agencies; other countries, individuals and businesses take part as well.

3.2 The firewall: Separating private from public

The first real separation between the public Internet and the private Intranets began around 1987, when so-called firewalls were first deployed [29]. According to Power and Fallow, a firewall is a machine or collection of machines between two networks, meeting the following criteria

- The firewall is at the boundary between the two networks;
- All traffic between the two networks must pass through the firewall;
- The firewall has a mechanism to allow some traffic to pass while blocking other traffic.

The rules describing what traffic is allowed enforce the firewall’s policy.

Note that this definition does not imply any different levels of security between the two networks. In practice however, firewalls were used to protect internal, trusted networks from the Internet. At first, the firewall could just be a single device or program, that separated a trusted system from the Internet. On the Internet, these firewalls were the first security perimeters.

3.3 Technological de-perimeterisation mechanisms

Since 1987 the Internet and its users have changed enormously and so did the security mechanisms that people deployed to defend their systems.
This gradually led to the disappearance of the idea of a single security perimeter. For convenience, we group these changes into two categories:

- Technological changes of the Internet and the systems that connected to it
- Changes in the way that organisations do their business.

Of course, these changes are not independent; Technological changes make new business processes possible; Developments in organisations place different demands on technologies which change in their turn.

**Network capacity increased: Greater reliability needed**

Firstly, the capacity and performance of the networks and the networked computers increased. A typical end-user modem in the 1980s had a speed of 1200 bit/s, but today some ADSL modems can achieve a downstream speed of 24Mbit/s, or 20,000 times faster. The consequence is that the firewall must filter much more data. At the same time, it became much more critical to filter this data. A well-used reliability standard is that of the five nines, a system has an optimal level of reliability if it is working 99.999% of the time. For a device, this means that there is an average window of 5 minutes and 15 seconds per year in which it will not function. This might not seem like a lot, but for a firewall, in the case of ADSL, close to 1GB of data can be transferred in this time window.

**Internal network size growth: Firewall distribution**

Another development was the increase in size of the internal networks, so-called Intranets. As a consequence, they became less trusted. Combined with the fallibility of firewalls this led to an approach of defence-in-depth with intrusion detection systems or IDSs. These systems would check Internet traffic inside the organisational network. In the early days of the Internet, these could consist simply of print-outs from audit trails that were checked by an administrator [21]. Later, automated and more complicated systems emerged, which complemented the firewalls. Also, organisations started to split-up their networks. Some hosts needed to be accessible from the Internet itself (such as web and email servers) and were placed in a special zone called DMZ or demilitarised zone [29]. The internal network was then protected by another firewall. Nowadays, many devices have firewalls themselves and do not rely on organisational firewalls to protect themselves. Again, these developments distort the idea of a single security perimeter.

**Network mobility and connectivity increase: Connection overload**

The way in which organisations connected to the Internet also changed. In the early days of the Internet, it was not uncommon for organisations to have just one connection. This changed into a situation where organisations have many different connections, for example to facilitate load-balancing and increased reliability. This adds additional complexity to the security perimeter. Also, the nature of the networks has become more dynamic. This is especially the case when we look at wireless networks. Devices such as laptops and mobile phones can connect to the Internet, independently of the corporate network that they supposedly belong to.

---

[^1]: According to the ADSL2+M standard
Encryption usage: Content invisible  In the mean-time communication protocols changed. Earlier, there were a limited number of applications and protocols that could be easily distinguished and filtered. If email was not allowed, it could be blocked. If file access should be possible, it was allowed. However, these protocols began to merge. Nowadays, protocols for web browsing, email and instant messaging can all send or receive files. Secondly, many of these protocols are using encryption, which ensures that traffic between two end-points cannot be decoded. This makes it hard for the firewall to do a content analysis on the traffic, and decide what it should let pass.

Unintended consequences: The connection paradox  Finally, we need to consider that Internet connectivity has become both a threat and a cure. This paradox started when the number of applications that required Internet access increased. Now that all these computers are connected, they became an attractive target for hackers. They would search for vulnerabilities in the software that could be exploited. This situation leads to frequent patches from software vendors. The time between the discovery of vulnerabilities and their exploits has decreased - and this, in combination with the increased amount of servers, led to automated patching: Systems frequently contact their vendors and check if updates are available. All this requires Internet access - to protect the servers from the same Internet that threatens them. Note the servers’ security also depends directly on the vendors: One wrong patch can damage many servers in very little time.

3.4 Organisational de-perimeterisation mechanisms

Low communication costs made it possible for organisations to utilise resources from outside of the organisation.

Remote access: Telework  A first consequence is that the organisation’s physical location and its business do not need to coincide anymore. Employees can work from home, using the exact same data that is available at the office. Sales representatives can stay connected to the main business network while being with a customer. It is debatable whether this is a real breakthrough caused by the Internet. Even without Internet access, employees can still do useful work on mobile devices when they are not connected. All that is required is some working data, that can be synchronised with the main branch once they are available at the office. However, improved Internet connectivity did increase the scale at which this happens. The connections blurred the security perimeter even more, because employees can be physically outside of the office, while they have access to everything inside it.

Outsourcing IT: mixed security zones  Secondly, the Internet made it possible to outsource and insource services on an unprecedented scale; that is, once they were encoded in a digital form. A good example is

4In fact, releasing a patch can actually increase the chance of an exploit - reverse engineered it will show what problem it was meant to solve - and thus reveal the vulnerability

5It is important to point out that an airgap does not provide ultimate security any more. Any useful system nowadays has undiscovered vulnerabilities. If it is not patched, it will not be protected against future exploits and will thus be very vulnerable when it is stolen. All that is needed for an attacker is sufficient time for the vulnerabilities to be discovered.
the outsourcing of IT maintenance itself. If an organisation could find no competitive advantage in having its own system administrators, it could outsource the jobs to another company. Their employees could then remotely access the network and perform the necessary maintenance. This organisation’s servers are in a mixed zone: They are not entirely inside the perimeter, but neither are they outside the perimeter.

**ASP model: Data stored externally** In the previous example, the organisation’s physical servers were still inside the organisation’s building, but that began to change. Organisations started to put applications for rent on the Internet as if they were services. This business model is called the application service provider model, or simply ASP. The consequence was that one organisation’s data would be under another organisation’s physical control. Again, the security perimeter blurred.

**SOA and virtualisation: Mixed security zones** How advanced the ASP model might be, it was not the end of the outsourcing development. As the number of customers for and ASP grew, it became difficult to satisfy all their requirements. A new feature that would be useful to one customer, would be a breaking change for another. The solutions was to offer more fine-grained structures or services. Other parties could then orchestrate these into new business processes on their services. This is the service oriented architecture (SOA) [30]. Other variants are called SaaS (Software as a Service) or PaaS (Platform as a Service). A final variant is virtualisation, where organisations can rent virtual servers on an on demand basis, of which the underlying hardware is maintained by yet other companies. Again, such systems represent a mixed security zone, for which there is no single company responsible.

**Business and employee dynamics: Flexible zones** The Internet also increased the pace in which business is possible. Organisations are not static themselves; they are restructured, taken over, they merge. People are no longer being full-time employed for one job; It is more common to work on inter-organisational projects for shorter periods of time, for example on a joint-venture. Thus the security perimeter becomes very flexible.

**Individual empowerment: individual perimeters** Another side effect was that the availability of on-line high quality applications led to empowerment of individuals. In many businesses, the Internet has lowered the barrier to entry until it was possible for individuals to work for themselves. In such a case, there is no organisational security perimeter - individuals secure their assets themselves.

**Cooperation without contract: vanishing security zones** In the previous paragraphs we saw some examples where organisations outsource or insource work; This is still done by contract. But in some cases, connections (and dependencies) between organisations and/or individuals function without any formal contract. This is the case for many search engines, on which many people depend upon for their work. On-line advertisements make it possible for websites to deliver valuable services at no cost to the customers. Some consider the Internet a public good [28], and maybe search engines can also be seen in that way. Where is the
security perimeter of a search engine, that scans the entire Internet and delivers results for free?

We list the developments in Figure 5.

<table>
<thead>
<tr>
<th>De-perimeterisation mechanism</th>
<th>Impact on security perimeter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network capacity increase</td>
<td>Firewall reliability must increase</td>
</tr>
<tr>
<td>Internal network size growth</td>
<td>Firewall distributed over internal network</td>
</tr>
<tr>
<td>Network mobility and connectivity increase</td>
<td>More gates, mobile gates</td>
</tr>
<tr>
<td>Encryption</td>
<td>Firewalls ineffective</td>
</tr>
<tr>
<td>Remote access</td>
<td>Separation of physical and digital perimeter</td>
</tr>
<tr>
<td>Outsourcing IT</td>
<td>Mixed security zones</td>
</tr>
<tr>
<td>Application service provider</td>
<td>Data outside security perimeter</td>
</tr>
<tr>
<td>SOA and virtualisation</td>
<td>Mixed security zones</td>
</tr>
<tr>
<td>Business and employee dynamics</td>
<td>Flexible perimeters</td>
</tr>
<tr>
<td>Individual empowerment</td>
<td>Organisational perimeter replaced by individual one</td>
</tr>
<tr>
<td>Cooperation without contract</td>
<td>No perimeters</td>
</tr>
</tbody>
</table>

Figure 5: de-perimeterisation mechanisms and their impact on the security perimeter

4 The dynamics of the re-perimeterisation cycle

4.1 Security impact

Obviously, as connections between systems increase in unknown ways, this has implications for the security situation for businesses. However, are these implications desirable or undesirable? Maybe de-perimeterisation is not a problem. After all, IT works very well in general; In fact, the occurrence of de-perimeterisation indicates that software and hardware are very reliable and that most people that operate their systems are trustworthy. Apparently it really does not matter whether your data centre is located in Europe, the US, India or elsewhere. There are security breaches, but a complete cascade failure of the Internet has not occurred yet.

However, with respect to security, de-perimeterisation does threaten organisations in several ways.

Dependencies are obscured  In a networked world, it is not hard to create very complex systems of systems, that work flawlessly for some time. However, these systems have structural dependencies that only become apparent when something goes wrong. For example, in 2007, Skype went offline for some time after a massive reboot of Windows machines, following an update. [31] Obviously, Skype was dependent on the patching process of Windows, but this was unknown before the event. How likely are such events in the future?

Risk assessment is hard  An especially challenging problem is risk assessment. For example the Common Criteria [7] uses protection profiles for specifying security requirements, as well as the concept of target of evaluation, for the system for which the risk assessment is done. In
many situations, these systems cannot be defined - we do not know what the requirements are and we have no idea what kind of systems we are dependent upon. That alone should be cause for concern.

Although IT systems are overall very reliable, we think that de-perimeterisation does pose some challenges to everyone that deals with IT security. The uncertainty of security increases and this makes risk assessment an especially challenging problem. It seems to be very difficult to do any kind of risk assessment when the boundaries between systems are blurred.

**Ineffective security mechanisms** First of all, de-perimeterisation reduces the effectiveness of security perimeters. We now examine the implicit assumptions behind the consideration to deploy a security perimeter P to protect asset A from asset B:

1. A is a valuable asset to some actor E
2. A can be located by E
3. A cannot protect itself
4. A is inside an threatening environment
5. It is desirable that A should be protected
6. It is possible to deploy P
7. P helps to protect A
8. P does not have too many negative side-effects for E (for example, in a business environment, it is still possible to do business).

Clearly, with de-perimeterisation, these assumptions are becoming more problematic.

1. In many cases we cannot locate the asset A, because it is not under our control or it changes frequently.
2. Many assets are deemed to be capable to defend themselves against threats, or the threat is unknown.
3. To assess the need for a security perimeter, we need to know the risk; However, we have little information on the asset and cannot assess the risk; In fact, we are not even responsible for its security.
4. We cannot always deploy a security perimeter around A because it is not under our control.
5. Many security perimeter technologies do not really help to protect A.
6. The security perimeter harms other business processes because it cannot be configured precisely enough.
7. Even after deploying, we do not assume that A is secure, for example because it is maintained by another organisation.

**Continuing need for organisational security perimeter** From a legal point of view, we argue that the organisational security perimeter should stay intact. After all, there remains a legal foundation for any organisation. Each organisation

- has ownership of certain assets
- employs personnel
- is liable for its actions
• can make profit
• has to pay taxes

Any useful security scheme should therefore deal with ownership, employer-employee relations and liability. The duties and benefits of an employee are tied to the organisation. A salesperson is responsible for selling a particular product or service and is paid by the organisation. This is regardless of where and how he works. Even outsourcing or off-shoring do not change these basic facts. In spite of de-perimeterisation, the concept of organisation does not change overnight. In fact, compared to the fast developments in IT, the concept of organisation has remained rather stable. Consider an innovative organisation such as Google: It may have its servers in many places in the world, serve as an application service provider to millions of people, but it is still defined as an Inc, located in Mountain View, having a notation on the NASDAQ.

If we “forget” that the organisational perimeter exists, and do not implement a security perimeter around it, this will cause a loss of control, which can have many consequences, such as a wrong allocation of benefits. Most obviously, the CEO of an enterprise cannot give an “in control” statement if he does not know which systems are part of the organisation and which are not. Note that the consequences might not be immediately apparent, as long as all systems work satisfactory. Only when problems arise, when systems go out or malfunction, it will become apparent that it is necessary to know which system was owned by whom and to whom its benefits should be allocated.

If the organisation is to function at all, the supporting IT infrastructure has to reflect its legal basis.

4.2 The re-perimeterisation cycle

Figure 6 shows the Jericho Forum’s view of the historical development of de-perimeterisation [18, p.1]. According to this model, the trend is toward more connectivity. However, our historical review shows that the real trend is closer to an oscillation than to a straight line.

1. Before the Internet all systems were separated;
2. Next they were connected;
3. Then firewalls separated them once more;
4. The internal networks (Intranets) grew;
5. The internal networks were separated;
6. Currently the networks are connected again

This situation is depicted in Figure 7.

The oscillation is due to the interplay of two sets of opposing forces, one in the direction of connectivity (de-perimeterisation), and one in the direction of (re)perimeterisation.

The forces in the direction of connectivity include the desire for cost reduction, flexibility and speed of business, facilitated by technological developments. Enterprises see the advantages of e-business and open up their networks. Consumers want to try out the latest available technology. Universities want to develop and utilise the new infrastructures for their own research. For many new technologies, their impact on security is not clear. Parties that are not aware of this, or do not consider it a problem,
will take the risk and adopt the technologies. Thus, there is no incentive to invest early on in security features.

Once technologies become mainstream, different forces come into play, leading to re-perimeterisation. Vulnerabilities will be found, and potential users will demand security features to be fitted to the new technology, before integrating it in their systems. Additional forces include the need for accountability, proper allocation of benefits in a business network, privacy, safety and reliability and company confidentiality.

Our prediction is that this oscilatory trend, rather than the linear Jericho trend, will continue. The reason is twofold: First, we think that for non-profit organisations and consumers, security is never a primary selling point for new and untested technologies. Secondly, we think that none of the forces in play will go away.

5 Re-perimeterisation mechanisms

The main question for re-perimeterisation is how to build effective perimeters, without undoing the positive effects of de-perimeterisation.

- what sort of perimeters should we build?
- around what assets should we place them?
- should the assets themselves be changed?
Earlier we defined de-perimeterisation to be about connections between systems owned or controlled different legal entities. From this we take it that we can solve it in two ways:

- Technical re-perimeterisation. Here we look for solutions to restructure systems and the way they influence each other.
- Organisational re-perimeterisation. Here we examine ways in which to restructure organisations and the way they influence each other.

These will be discussed in the next sections.

5.1 Technical re-perimeterisation

In this section, we look at technical measures for re-perimeterisation, trying to find out where we can put an effective security perimeter in place.

We will discuss putting perimeters around networks, data, endpoints, the entire Internet as well as layered solutions.

5.1.1 Network perimeters

Network or firewall security allows us to limit data flow between different systems, by inspecting and filtering the traffic that goes between them.

There are two typical scenarios: In the first, we need to protect an asset against outside influences, in the second case, we want to prevent information from leaking into the environment. Apart from packet level
firewalls there are also application-layer firewalls, with can filter traffic at the application-level. For example, we can filter email traffic and spam can be returned directly at the border of the organisation. Vice versa, emails can be scanned to prevent sensitive information to be communicated to outsiders. Other examples are XML-firewalls used to filter and route messages between different services in a service-oriented architecture (SOA) environment.

The Jericho Forum [14] has argued for their abolition, claiming that they hinder business rather than support it. Earlier, we saw how firewalls became less and less effective, due to increased and encrypted traffic. A requirement for such forms of security is that the network infrastructure must be under control of the organisation - in a de-perimeterised world, encryption must be regulated, such that the traffic can be inspected at the perimeter.

5.1.2 Data perimeters

One of the relatively new ideas to battle de-perimeterisation is to place a perimeter around the data, rather than around the entire infrastructure of the organisation. The Jericho Forum has argued for this protection scheme in their commandments [16]. The technical mechanisms are proposed in two key articles by Agrawal et al. [1] and Grandison et al. [12].

There are several arguments for implementing security on the data itself. A first argument is given by Grandison et al. [12], who state that security must be data-centric because only the data has real business value: The network of an organisation is of no serious concern if there is no sensitive data on it. A firewall is unnecessary if there is no risk of a security breach.

Secondly, it does not make sense to have a security perimeter include more than is strictly necessary. In general, perimeters do not scale. In addition, they tend to be less meaningful as the inside of a security perimeter increases in the number of assets to be protected. When the inside increases, the difference in security levels between the inside and the outside diminishes: On a network of 10 servers all of them could possibly be trusted, but this is not the case if the network is expanded to include a thousand servers. Intrusion detection systems do not really solve this problem.

A third argument is about business opportunities. The Jericho Forum [14] argued that organisation-level security perimeters actually hinder business rather than facilitate it. Security is in many cases not the goal. Often, profit is more important and security must be cost effective. Security is about risk management and opportunity costs: If you try to close down the network (ineffective as it may be), how many business opportunities are lost? To enable cooperation with other organisations it makes sense to facilitate access to IT assets at the lowest possible levels, and use these assets as building blocks for new business constellations.

Fourthly, if we compare the organisation to its data, we can find that an organisation can change shape quite often, but the data will remain relatively stable. For example, a hospital might be reorganised and restructured many times, whereas the patients and their data will remain fixed. Putting security policies as the data level can be a form of future-proofing security. Wherever the data will be in the future - it will be known how they should be secured.

Conceptually, we see several branches of data-level security, one im-
implemented at the level of a database, one implemented at the level of particular data items and one where data is simply encrypted.

There are three main forms of data level security: database centered, sticky policies and encryption.

**Data level security - database centered** The illustrative example here is the Hippocratic database [1]. It takes its name from the Hippocratic oath that doctors must take to protect their patients and keep their information confidential: Ideally a database should adhere to the same principles automatically. A Hippocratic database has an extensive set of tools to implement the required security policies. For example, it would support K-anonymity and certain obligations. On top of this database other applications can be built, that automatically comply with all security policies.

**Data level security - sticky policies** In contrast to the Hippocratic databases, where the data is stored centrally, there is the idea to allow free movement of the data but enforce its security at every location. Here, a data item is always associated with the policies that should be followed. These sticky policies [2] cannot be separated from the data items itself. DRM technology can be considered an example of this scheme. For sticky policies to be effective, it is usually required to have a trusted environment in which the data can flow: Policy enforcement is sometimes done with the help of special hardware.

**Data level security - encryption** Another approach is to encrypt data inside the database. For example credit card numbers are encrypted. (This is actually one of the requirements of the PCI standard [6, p.5].) Users that need access to the data need a key to decrypt it. Some systems also make it possible to search through the data. The server might store a text in encrypted form, and users can search for particular phrases. The server is assumed to be “honest but curious”. Extra precautions must be taken to prevent the server from learning too much about the plaintext.

**Limitations** Often, the smallest encapsulation of organisation-owned data will necessarily encapsulate items at the organisational level, taking us back to the organisational security perimeter.

As a practical example, consider the security system for a banking application. Among other things, the security concept includes data integrity. Now it seems that data integrity here cannot be determined at the level of individual bank accounts. If a sum of money is transferred between two accounts, integrity is at least determined at the level of those two accounts: The total amount of money before and after the transactions should be the same. In fact the expected level will be substantially higher:

- The calculations done in transferring data between accounts are done by an application. For example, banks tend to retain money between transfers for some time, which results in lower interest for their customers. The retention time and interest rates are not determined by the individual accounts. This indicates that security must be dealt with at the application level.

---

6Both the data-centric security approach and the Hippocratic database were developed by IBM

---

20
• It is the bank that is accredited for performing financial transactions. For this accreditation the bank will have to prove its operations are valid. This is again a drive toward having security determined at the organisation level.

Three basic facts that data-level security cannot deal with are:

Organisations do not cease to exist. For legal reasons alone, we need to know what is inside and what is outside of the organisation. This is an "undocumented" but essential function of the security perimeter.

The security of data itself cannot be assessed. Computational processes (and the applications, and the business processes) are what makes the data secure in the first place. We cannot assess the security of data at face value, we need to know with which applications it was generated and by whom.

Data needs to be exchanged with other systems Communication of data to other organisations and individuals is a necessity: The problem of maintaining a secure data exchange cannot be addressed at the data level.

If we are to see a move toward a more open architecture, we can expect more from SOA (Service Oriented Architecture). Here an application is structured as a set of services that can be accessed by many parties, potentially outside of the organisation. Each of these services can be configured for optimal security. If the bank properly aligns its business and IT systems there will be only one such security service that will closely match the organisational perimeter.

Generally, most data-centric solutions are aimed at data confidentiality - but are less well suited for improving integrity and availability.

5.1.3 Endpoint perimeters
The principle of endpoint security dictates two things:

• When there is communication between two nodes (or endpoint), each node is responsible for maintaining its own security
• Communication between the nodes is secured

If required, policies for endpoints can be centrally managed. Forms of endpoint security are personal firewalls, anti-virus software on client PCs, VPN and SSL/TLS connections.

In the case when the network infrastructure is fragmented and communications between nodes are ad-hoc, endpoint security limits the security implications: The network (apart from reliability) does not have to be secured anymore.

Ideally, each endpoint is a very simple system which is easy to secure. Unfortunately, for an end-user, an endpoint normally means a PC, which is so complicated that it is not reasonable to assume its security in many cases. It is also a single point of failure - once one the endpoint is hacked the security of the entire network is completely breached.

5.1.4 Multi-layer perimeters
In multi-layer security, there are different zones that each have different security levels. Typically, the inner-most part is the best secured part. In
situations where services are outsourced, this model can be extended \[35\] to include an extended security perimeter. We also see similar situations where firewalls are used; The inner parts are then protected by several shells of firewalls.

The reason for using multi-layer security is that there are distinct parts of a system or organisation that need to be better secured than other; while the parts that surround it are also under the control of the organisation. As such, it allows for defense-in-depth. (If a public accessible webserver has to be secured, the concept of multi-layer security might not be of much use). Multi-level security is a defense-in-depth approach to security. As such it can help to counter de-perimeterisation.

In the multilayer security model defined by Walker \[35\], the security is split into four parts:

- Electronic Security Environment (ESE)
- Local Security Environment (LSE)
- Global Security Environment (GSE)
- Extended Security Environment (XSE)

In the ESE, the assets are databases and applications, the mechanisms is endpoint security. The LSE has a firewall and defines policies and rules for auditing. The GSE is the outer organisational perimeter. The XSE is the trusted environment outside of the organisational area of control.

The drawback of multi-layered solutions is that they can become very complicated, especially when a layer has to be partitioned itself, for example because each business partner requires its own environment.

5.1.5 Internet perimeter security

A more radical approach is to put a perimeter around the entire Internet. Such an approach is for example foreseen by Lessig \[23\]. “Ideally”, Internet access is restricted to those systems and individuals that have identified themselves properly. There have been a number of initiatives that would support such an architecture. So far, only building blocks have been developed, including IPV6, identity management systems and trusted computing chips.

With a functioning identity layer, trust becomes easier to organise, as organisations do not have to build the trust network themselves.

Realising such a perimeter around the whole Internet is unfeasible. First the entire infrastructure needs to be changed; Secondly there is a privacy problem: identifying everyone and every device means that privacy is lost. Thirdly we need to take into account existing laws in all countries connected to the Internet. So far, attempts to create even limited forms of identity layers (such as Microsoft Passport \[26\]) have failed.

5.2 Organisational re-perimeterisation

We will now move to the organisational measures for re-perimeterisation, trying to find out how we can rearrange the responsibilities of different legal parties involved.

5.2.1 Organisation perimeters

Here we try to partly undo some of the causes of de-perimeterisation. For example, when the management of applications was outsourced, it can be insourced again, and placed under control of the organisation.
<table>
<thead>
<tr>
<th>Technical re-perimeterisation mechanism</th>
<th>Conditions</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network perimeter</td>
<td>Network and protocols must be controllable</td>
<td>Cost, complexity</td>
</tr>
<tr>
<td>Data - database centred perimeter</td>
<td>Processing is less important than storage</td>
<td>Mostly useful for confidentiality</td>
</tr>
<tr>
<td>Data - sticky policies perimeter</td>
<td>Environment is trusted</td>
<td>Mostly useful for confidentiality</td>
</tr>
<tr>
<td>Data - encryption perimeter</td>
<td>Processing is less important than storage</td>
<td>Mostly useful for confidentiality</td>
</tr>
<tr>
<td>Endpoint perimeter</td>
<td>Endpoints can be secured</td>
<td>Single point of failure</td>
</tr>
<tr>
<td>Multi-layer perimeter</td>
<td>Ability to manage complexity</td>
<td>Complexity</td>
</tr>
<tr>
<td>Internet perimeter</td>
<td>Privacy and legal problems are solved</td>
<td>Not feasible</td>
</tr>
</tbody>
</table>

Figure 8: Technical mechanisms and requirements

The main advantage of this approach is that it reduces the amount of legal parties involved. This perimeter type is typically used in financial institutions and governments. There, certain risks are simply unacceptable and must always be treated, and cost is less of an issue. Organisational perimeterisation can be done on the condition that the organisation has control over its network and has the available expertise to maintain it.

The biggest problems with this solution are cost and lost business opportunities: It can be very difficult to manage applications properly, it required highly trained and expensive personnel. This also holds true over time: Once a system is hard to maintain, it is also difficult to upgrade or replace and the organisation cannot benefit from newer solutions. Secondly, and organisational perimeter hinders external communication with partners and thus results in lost business opportunities.

5.2.2 Individual perimeters

It could also be possible to maintain security under a dissolving organisational security perimeter using another method: By making every individual responsible for keeping himself and his own devices secure. Already in [13] it was observed that security was moving into this direction. The idea is explored here in to more detail. A system is said to be using individual centric security if the burden of maintaining security is put down on individual users. They are responsible for keeping the system up and running and have to make decisions with security implications. These implications are usually (and ideally) limited to the user himself. There is not necessarily a central or higher authority involved.

The main rationale is that in many cases, there is not one organisation that can provide oversight or control. The world is simply too complex and it would be too expensive to management systems centrally. Instead, people place trust in each other.

- Individuals work in multiple organisations, on joint projects
- Individuals have their own personal IT infrastructure
- Individuals manage their own work
- Individuals own data themselves
• Individuals can manage their own IT infrastructure

It can be argued that the only reason for centralised administrative control is when ownership does not coincide with individuals. If a person works on his own laptop on his own project, on his own document, in his own free time, there is a perfect match and no organisational security perimeter is needed.

An example of the shift towards individual centric security is the trend to replace shared PCs by individual laptops and mobile phones: Rather than having a uniform set of desktops in place, where everyone can login at any PC, organisations are now shifting towards a concept where users all have their own laptop. Rather than using shared land-line phones in the office, users now carry their own mobile phones with them. Each user maintains his own system and has to make sure he installs patches regularly, make daily backups etc. Another example is a peer-to-peer file sharing system, where users exchange data with each other, based on a certain protocol. Each user can search and download files - but cannot make decisions affecting other users or influence resources that he does not directly own. Skype [3] can also said to be using individual centric security. Individual users communicate through it, sign up for accounts, invite others to participate in their communications. In general, Skype will not care much about user security of accounts, data loss etc., as long as the Skype service can still be used. Skype communication is supposed to be secure - but everything else is up to the users. Some systems that store medical information also use individual-centric solutions for example Microsoft HealthVault [25] or Google Health [11]. Here individuals can manage their own medical information and decide themselves who will get access to these records (for example which doctor or which family member).

There are some situations when ownership and control will never coincide with individuals, and individual centric security is not possible:

• Working as a factory worker on a conveyor belt
• Doing a bank transaction for a company as an employee
• Using a collaborative resource such as Blackboard or EPrints.
• Working at a company during office hours: The company can demand that some applications will not be used.

Organisations are a natural way to structure economic activity (Cf. Coase [4]). It is impossible to think of building a passenger aeroplane alone and every employee in a firm will have some form of administrative control imposed on him. In such cases, individual centric security is at odds with organisational alignment.

A specific disadvantage is that individual centric security has a tendency to mutate into other forms of security.

• In the healthcare domain for example, if a medical file would be controlled by one patient, he still has to give some authorisations to a hospital, because he cannot authorise all nurses individually.
• As for Skype, its underlying infrastructure will have to be managed somehow, and this will probably not rely on individual centric security.
• In social network sites, basically connections of individuals, organisational accounts appear, which do not fit well into the individual centric concept. For example, Warner Bros, a multi-billion dollar
A company, has its own user account on YouTube called “warner-brosrecords”. This leads to the conceptual problem of which employee (or employees) of Warner Bros has access to this accounts, and whether user rights are managed by either Warner Bros or by YouTube, since no single Warner Bros employee owns the rights to a video clip.

Another problem is that individual users might not be capable of securely configuring their systems. In the case of medical files, users might need to set authorisations to all kinds of doctors, check the audit trails for unauthorised access. A user has to maintain its own laptop, install patches, configure the firewall etc. etc.

5.2.3 Virtual organisation perimeters

Whereas with federated systems organisations agree to exchange data, with virtual organisations [27], we can create a new organisational structure between the organisations themselves. Employees of different organisations can become a member of this virtual organisation.

Effectively, this reduces the amount of connections between different legal entities. An example of virtual organisation usage is in grid computing. Here, different institutions cooperate in using resources from yet other organisations or even individuals. By combining the institutions into one virtual organisation, the resource owners only need to deal with one organisation. Another typical case is when companies have an outsourcing relation and create a separate unit to monitor a service-level agreement. In order to use virtual organisations, initial trust in other parties is required.

A negative aspect is that a virtual organisation is another organisation, and can thus also introduce new complexity and connections, because employees might now be a member of two organisations rather than just one.

5.2.4 Federated perimeters

Another solution direction is to use federated systems [10]. If security cannot be addressed on the organisational level, it could be implemented at the inter-organisational level, by putting a security perimeter around multiple organisations. In a federated solution, several organisations agree to use a shared security solution, the features of which can be used by all participating organisations.

A federated solution can help in difficult security situations such as ‘person P works on a website that is owned by organisation X, on data owned by organisation Y from a computer owned by organisation Z’. Federated systems can especially help with identification and authorisation. If someone is identified at one organisation, he can use his credentials at another organisation. A specific case is when the federated solution is provided or even mandated by the government. Federated systems scale very well. In a network with N systems, we only need one extra connection from the root system to a new system. Where the network built on an ad hoc basis, we might need to build N different connections. The advantage of federated security is that the amount of connections between organisations can be reduced drastically. Examples of federated solutions are Microsoft’s Windows Live ID and its Active Directory where management domains can be placed in a hierarchical relation (so called forests).
An example of a government identification scheme is the Dutch DigiD system [37].

The main problem is that we need to rely on a centrally managed site. If multiple organisations want to work together they must come to some form of agreement. There could also be legal problems, when organisations cannot share their data.

**Overview of all mechanisms** We will now list all mechanisms and the requirements they impose on correct implementation.

<table>
<thead>
<tr>
<th>Organisational re-perimeterisation mechanism</th>
<th>Conditions</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation perimeter</td>
<td>Expertise, control</td>
<td>Cost, lost business opportunities</td>
</tr>
<tr>
<td>Individual perimeter</td>
<td>Control and ownership rest by the individual, expertise</td>
<td>Insecurity</td>
</tr>
<tr>
<td>Virtual organisation perimeter</td>
<td>Cooperation is possible</td>
<td>New complexity</td>
</tr>
<tr>
<td>Federation perimeter</td>
<td>Cooperation is possible, trust</td>
<td>Loss of control</td>
</tr>
</tbody>
</table>

Figure 9: Organisational mechanisms and requirements

### 6 Discussion and further work

We have defined the concept of de-perimeterisation and shown that it is not a steady process, but a cyclic one. In one cycle, different forces accelerate de-perimeterisation, after which other forces slow it down, leading to re-perimeterisation.

We derived that there are basically two methods for “re-perimeterisation”:

1. We can put technical security perimeters around different parts of IT: for example around data, around endpoints or try to use a multi-layered approach.

2. We can re-engineer the legal constructions in which the systems function: for example by focusing on individual responsibility or creating virtual organisations.

Together the options provide a framework that IT and business architects can use together for developing secure, re-perimeterised solutions, which can survive in today’s networked world.

In the future, we would like to investigate how technical re-perimeterisation options can be combined with the organisational options. So far, we have only sketched the requirements and limitations of each individually.

Physical security was not discussed in this paper. We plan to investigate this further. Also, we can apply additional perspectives on de-perimeterisation. The first concerns identity - one of the recurring problems in de-perimeterisation is identification - often it is a precondition for trust. When organisations are cooperating, they need to know with whom and with which IT systems they are dealing. This view is also related to the emerging discipline of context-aware security: security depends on the context and the context is described in terms of identities, such as buildings, persons, information systems. Much of this information is missing.
now, and de-perimeterisation can thus be seen as a step in the process of embedding physical and organisational context inside of IT.

References


List of Tables

List of Figures

1. Perimeter and environment ........................................ 8
2. Security perimeter model ......................................... 9
3. Perimeter and environment ........................................ 9
4. Security perimeter definitions ................................... 9
5. de-perimeterisation mechanisms and their impact on the security perimeter ........................................ 14
6. Trends according to the Jericho Forum .......................... 17
7. Alternative view ..................................................... 18
8. Technical mechanisms and requirements ........................ 23
9. Organisational mechanisms and requirements ................... 26