P7

Unite Security Culture

May a unified security culture be plausible?

Rauno Kuusisto
Finnish Defence Forces, Finland
P.O.Box 7, FIN-00861 Helsinki, Finland
rauno.kuusisto@mil.fi

Kaj Nyberg
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
kaj.nyberg@hut.fi

Teemupekka Virtanen
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
teemupekka.virtanen@hut.fi

Introduction

The aim of this paper is to study, whether a unified security culture is possible in culturally divergent environments. Security is considered as a whole, but the focus is set on the socio-cultural viewpoint. Long-term aspects of security are stressed. The meaning of security culture forming is discussed and some possibilities to create a holistic security cultural atmosphere are discussed. The problem is approached via Habermas' (1984, 1987) communicative theory, Hofstede's cultural findings (1984) and von Solms' (2000) thoughts about comprehensive concepts of security culture.

Habermas created the theory of communicative act in the 1970's. This theory expresses that an interactive social system is transferring information on four levels. Those levels determine components of action orientation. Components consist of values, norms, goals as well as means and resources. This paper focuses on values which according to Habermas are producing the function of pattern maintenance, and on norms, which function is integrating activities. Culture is a knowledge-based system that causes mutually accepted patterns of activity. It determines the basic background on which all activity will appear. Norms will determine the desired act of the members of society. In a multicultural environment, basic cultural assumptions may juxtapose

and mutually understandable norms will be necessary to form an accepted security culture in an organisation.

Security culture is considered via the work of Chia, et.al (2002), Schlinger & Teufel (2000) and von Solms (2000). Mono-cultural experiences from one organisation and studies concerning multi-cultural environments are compared against Hofstede's cultural dimensions. Finally problems in forming a unified security culture will be pondered from the basis of Habermas' classification of communicated information. The communication of values is also discussed.

The hypothetical departure of this paper is that a unified security culture is in the range of what is possible to achieve in a multicultural organisation. The research approach is hermeneutically pursued to gain understanding about the process of forming a culture. Research is completed by first explaining the main content of Habermas' theories about social systems. Aspects of security culture are combined to these theories. Secondly discussion about different cultural environments is done. Finally we will ponder what information shall be communicated to gain unity in a security culture and what kind of problems will arise during the process of forming the culture.

Keywords: Security culture, time-divergent communication, communicative theory, holistic security view

1. Social system and relevant information

Habermas bases his thinking on relevant information in the theories of social sciences. He is combining the theories about society, a human being as a part of the society, and system theories. (Habermas 1984, 1989) This approach will fit rather well into organisational and inter-organisational environments, as well. Habermas states that there are four basic classes of information, which are directing an actor's activity. These are values, norms, goals, and means and resources. These same basic items can be found from the background of any purposeful act at any level – from individuals via working-groups to organisations, from individuals via families to societies. Those items contain information, which – when used – will orient an actor to adapt its behaviour to better fit into the surrounding. In other words, the actors in a system will

interact with each other via exchanging various types of information. This information concerns values, norms, goals and means and resources. This information is fulfilling the demand of functions about pattern maintenance, integration, goal attainment and adaptation. Table 1. depicts these dependencies.

Table 1. Information concerning action orientation and functions in a social system. (Habermas 1989, 243, Figure 32)

Information concerning action orientation	Functions that will use the information
Values	Pattern maintenance
Norms	Integration
Goals	Goal attainment
Means, resources	Adaptation

Figure 1 describes a systemic approach to action. It describes what kind of information is flowing in the divergence of activities framed by certain structural phenomena situated in space and time. Information concerning values will determine a general subsystem of culture. The function of culture is to maintain certain patterns of activity. These patterns consist of cognitive interpretation schemes, symbolic expressions and value standards, like standards of solving moral-practical and cognitive-instrumental problems, as well as appreciations. Cultural orientations are both normative and motivational, the first containing cognitive, appreciative and moral and the latter cognitive, mental-emotional and evaluative. (See more from Parsons 1951, whom Habermas (1989, 216 – 219) is referring.) Information about values forms the long-lasting basis of information creation. Information about values is changing rather slowly and it is more or less dependant on the culture of concern. (Bell 1998, Hofstede 1984, Schneider & Barsoux 1997)

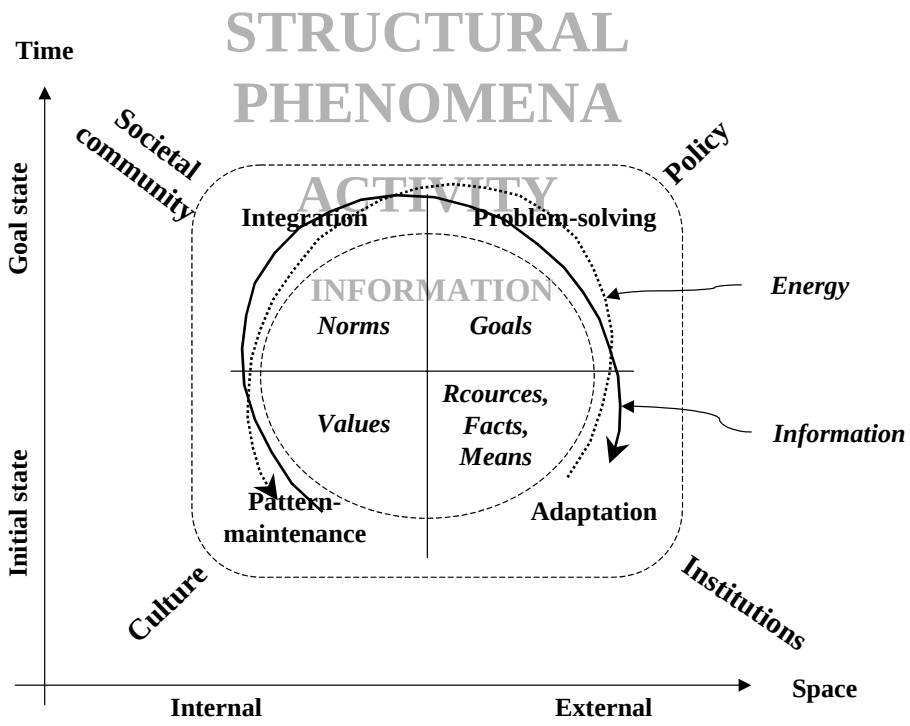

Figure 1. Systemic approach to activity in a social system.

Norms will determine mutually expected rules, among which the subjects of community will perform their interactions. Norms will entitle the members of community to expect certain actions from each other in certain situations. That will obligate members of this community to meet the legitimate expectations of others. Norms will build up a system of controls and orient actors' activities to fulfil normative validity claims. The acceptance of norms will lead to full adaptation and further development of patterns. (Habermas 1989, 32 – 42) The understanding of norms without acceptance will lead to various ways of action from seemingly total adaptation in the context of norm-setting community to total ignorance of norms and drifting outside of that community. The latter will happen, if norms are not understood, as well. There, the dilemma of subjective and objective world will be seen. The adaptation to the community will depend on the value-based judgement of the acceptance of those norms, which are set by the community.

Goals will determine the desired end-state of actions. Goals are directing resources and means to gain success as effectively as possible. Goals will provide information about politics, about the

choices, which are made by top management of one actor. This actor can be e.g. a state, an organisation, a team, or even an individual. Finally, means and resources are used to put such actions in practice, which will lead to the actor fulfilling its goals as optimally as possible. The user of those resources is here called an “institution”. Originally in Habermas’ theory, this structure is economy. Anyhow, it could be thought that depending on the viewpoint, this resource-using structure may just as well be something else. E.g. from the viewpoint of defence at a national level, this institution will be the defence forces. From the viewpoint of an enterprise, the institution will be e.g. marketing, production, and/or research and development department.

The circular arrow, which is named “information”, describes the direction of information, which is coming in to the information refining process. It shows that values have effects on norms, which both have effects on goals and the attainment of those, and further on all those have effects on using resources and means. Vice versa, the arrow called “energy” describes those activities, which are taking place from using resources to changing values. An actor has a certain variety of resources, means and facts to put in practice to achieve goals. (Habermas 1989, 235 – 250) Information is coming from the past and energy is pointed towards the future.

The structural phenomena of this systemic approach contain culture, community, policy and institutions. Information flows and actions described above will take place in these structural phenomena, which are subsystems of the whole system. They form an ontology as well. Cultural systems are more solid than societal systems, which are again more solid than political. This ontology may be applied to organisational environment, as well. Organisational culture will remain at least partly in spite of organisational changes, both ontological and normative. Policy, which determines goals, will change among the demands of the surrounding environment and information offered by norms. Finally, using resources and means will be mostly dependant on goal setting.

Over time, the system depicted in figure 1. will attempt to reach a goal state, which contains a normatively unified community, which is setting mutually accepted goals in policy process. This state will be constructed on cultural structures manifested by communicating values, and on the use of available resources. The system shall be able to maintain itself both internally and

externally. Information concerning values and norms will determine the interaction against the system itself. The system, whether it is e.g. an organisation or society, contains information about values and norms. This information will guide goal forming and the use of resources. Information about goals and resources will guide the social system to perform suitable interaction with the outer world. (Habermas 1989, 234 – 245) Culture can be seen as a structural phenomenon, which aim is to maintain suitable patterns of a social system to form a solid enough basis for orienting towards the future. Culture is communicated by values. On the other hand, Edgar Schein (1992) defines culture as a model of basic assumptions, which is invented, found or developed while learning to deal with those problems, which concern either the internal integration of organisation or its adaptation to outer challenges. This model is good enough to be justified and therefore valid to be taught to new members of an organisation as a method to perceive, think and feel. Definitions of culture by Habermas and Schein are not so far away from each other, but their perspective differs. When referring to figure 1. the functionality of culture forming process, which Schein is describing in his definition, can be found.

According to this thinking, a continuous process of the evolution of values and reconstruction of norms will be present in the system itself. Affecting the objective world will be done by policy-making and institutional structures. In an organisation environment, this means the will of the top management, and the optimal use of organisational resources, like information, time, material, personnel and money. Interaction takes place in a situation via a communicative process, where information about various items is shared between subjective actors using mutually understood codes. The whole interacting process is a series of situations, where mutual adaptation of interacting actors will take place.

2. Security culture

Organisational security culture is most obviously a part of organisational culture, which concerns both internal and external security aspects of an organisation. The development process of a security culture can be seen equal to any culture forming process. When referring to Habermas' theory, forming a structure called culture will require a lot of energy. If it is thought that energy

will be transferred via information, a subsequently great amount of information will be delivered. Therefore it will demand some amount of time to perform changes in cultural structures.

Dhillon (1997) stresses that the majority of security research has been dealing with technical aspects in a rather functionalist spirit, where positivistic approach to science has been conducted to normatively regulated environments. Schlienger and Teufel (2000) propose that a paradigm shift should be done from a technical approach towards a socio-cultural aspect. Von Solms (2000) claimed that the security culture tries to solve the "my user is my biggest enemy" syndrome. This syndrome may appear more frequently in multicultural organisations because of cultural differences. (Martins & Eloff 2002) Multicultural organisations may face severe problems, if security is understood differently. This will happen in a mono-cultural environment, as well, if security aspects are not understood and accepted mutually.

Security is somewhat complex concept itself. Teemupekka Virtanen is analysing in his thesis (2002), what security might be. He states that security has several viewpoints and he nominates the following ones. Security is:

1. Emotions from the subject's point of view. An individual likes to feel secure, because the thinking of a human being is combination of facts and emotions.
2. A profile as a part of every product and service.
3. Cost.
4. Optimisation to gain the best possible result in the complexity of benefit and losses.
5. A conflict between individuals and organisations.
6. Preparedness to anticipate possible risks and reject them in advance.
7. Bureaucracy to administrate all necessary tasks properly.

According to Jayaratha (1994), whom Virtanen (2002) is referring to, information security function contains information processing and usability, educational and learning, information system development, management and control, and strategy and planning. As been stated in the first chapter, the function of culture is to maintain patterns of activity concerning symbolic expression and value standards on normative and motivational levels. Culture is something that

exists within a subject. This subject can be an individual, but an organisation or a society as well. In this paper we will focus on organisational unity in security activities. If we refer this question to Virtanen's list presented above, we will notice that all of those are more or less dependent of the cultural environment.

Security is understood differently in different cultures and security can be approached via a divergence of viewpoints. Let us take an example about confidentiality via examples of personal privacy and governmental legal norms. With “corporate confidential”, we in the western culture understand that is something that must be kept secret and within the company. E.g. in the Asia Pacific, confidentiality is that sense is an unfamiliar concept. (Tam 2000) The concept of personal privacy diverges from the occidental one, which may astonish this western partner, who has been culturally familiarised to the nearly absolute respect of privacy. Normative differences concerning privacy will explain the effects of social engineering, as well. (Anderson 2001, ch. 3) The weaker the respect for privacy is, the easier it is to perform social engineering. The personal privacy is not only to blame. E.g. the US government has a somewhat strict attitude toward encryption technology and it will not easily approve such encryption methods, which are too difficult to break. (Anderson 2001) While attitude to security in the former case was determined by long socio-cultural patterns, the latter determines it via a regulative act.

The corporate culture determines how the nature of reality is seen in the organisation. According to Habermas’ theory, culture is the structural phenomenon, which will act as a platform, from which the information about the basic nature of the organisation will rise. (See figure 2.) On the other hand, culture will be the ultimate structural frame of the memory of the organisation, where all that information, which is considered the most valuable and preferable, is stored during the entire life on the organisation. So, culture is a structure, where the most long-effecting information, i.e. values of the organisation will be stored. When referring to figure 1., it could be seen that the energy to form the cultural structure will come via norms. Norms determine those rules, which will be followed inside the organisation to be able to work together as smoothly as possible. Norms and values are the inside information of an organisation, but they will be shown outside by performing activity via those goals that organisation has. This means that the values of the organisation will be communicated to the surrounding through its activities. It is rather

obvious that if a divergence of ambiguity of basic assumptions of an organisation will occur, its activity will be seen as inconsistent. It is rather easy to imagine, what will be happen to an organisation, which gives an obscure image about its activities on the security front. It shall be stated that a unified image regarding security aspects must be communicated towards customers and other organisations that interact with the organisation. Otherwise the organisation will not be very credible. Especially if it acts in such business, where security is essential.

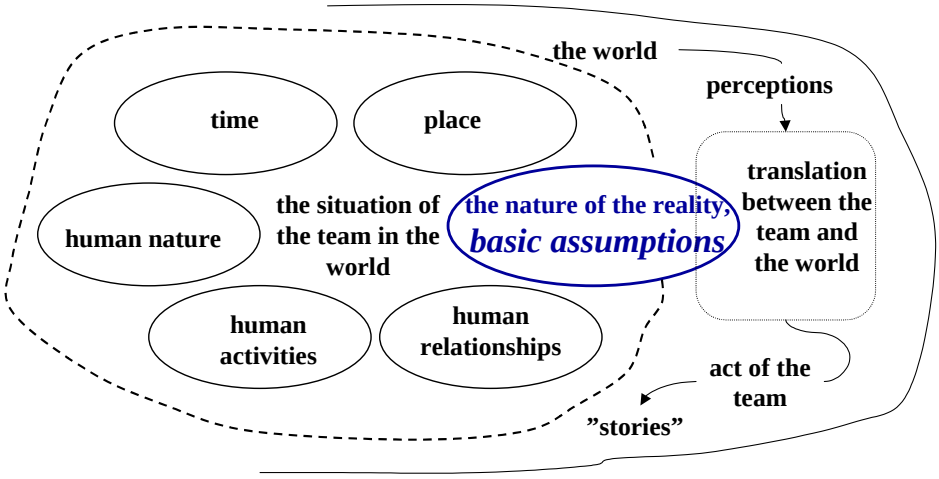

Figure 2. Culture forms the basis of interpreting information between the world and the team according to (Schein 1992). (Kuusisto & Helokunnas 2003)

People will do things like they have always done. Especially in the western world it is very hard for a company to determine, how people should valuate the world. The organisation has two main possibilities to create unity on the cultural level; it can choose its employees according to such criteria that the values of employees will match the values of the company or it can focus on combining the divergence of values of employees with its publicly stated values to form a foundation for a unified security culture.

3. A small homogenous company – an easy example

The case study was completed in November 2003 by Kaj Nyberg at Tekla Corporation. The company in this case study has some 420 employees of which one fifth works in subsidiaries in Europe, America and Asia. The company has one business area developing military technology

thus having strict demands of security. This unit is situated in Finland and all of its employees are Finnish citizens. In that sense it is special for the whole corporation. The customer (the Finnish Defence Forces) has set strict *norms* for security demands and supervises the adherence of those norms, as well. The security *policy* has been revised and refined over the years and many of those people, who were involved in forming the original security culture of the unit some ten years ago, are still employed there. The case study is based on interviews and personal experience gained under a period of four years. The personal values of the interviewer have been set aside while critically observing how the co-workers interact and behave.

The people currently working in the unit seem to have the same basic set of values. All are Finnish citizens, they are well educated, they have a technical background and they do not object to developing military technology for the national defence. The unit is rather small, consisting of 25 people aged 23 to 51. The turnaround of personnel is very low. One of the key values of all employees is patriotism. This cannot act as a basic value in multinational or multicultural organisations. Patriotism is a value of orienting loyalty. In this nominated case the basic value of employees fits very well to the customer relationship of the unit. All three main actors – customer, organisation and employees will prefer the same basic cultural structure. This is most helpful, when forming a unified security culture, as well. As a matter of fact, no security breaches have been reported during the working history of this unit. How has it been possible to create such unity in understanding the necessity of security? The answer is communication on a mutually understood value base. A senior department manager is in charge of security and the general principles of security are discussed continuously. Any new suggestions to improve security are taken into account and discussed among employees. They are encouraged to come up with security improving ideas.

The fact that we are dealing with a fairly homogenous group, not a multicultural one, makes the value-based approach that much easier to conduct. We do not have to worry about technical solutions that someone might find repelling or refuse to use just because it is “difficult”. We do not have to worry about how basic concepts like “confidentiality” are understood. Actually the normative layer, which integrates all members of the unit to act in a mutually accepted way, is not needed to justify continuously, because the value-base is basically the same for all people.

Norms will have the same base of understanding and therefore they are not obligated to be explained thoroughly after they have been understood the first time. Younger team members will learn norms and values of the company from senior members during informal meetings. This communication process is continuous and long-term information, like values, will have a good platform to take root because of low turnaround of employees. With learning comes respect and the values of the company are passed on to the younger generation. From a security point of view, this gives continuity, which is independent of technology. The support from executive management is strong and everyone at the department feels responsible for security. The employees understand that if security norms are not fulfilled, there is no basis for business. These findings are rather similar to that of Chia et. al (2002). Without support from top management and without understanding why security is important, we cannot have security at all.

In this case, some interesting features can be found. The value bases of the customer, the company and the employees were rather unified. Security demands came basically from outside the company. The customer had performed certain norms, which determined somewhat strictly, how security aspects must be dealt with. Security policy was determined by combining two essential items; the demands of customer-determined norms, and the company resources, which were usable to perform needed security activities. Norms and values were communicated in a continuous process inside the unit. Habermas' theory stresses that a society will orient to plausible future via mutually accepted norms, and perform activities determined by goals (compare to figure 1.). The basis for this process is in values and those resources, which are usable. Most interesting is that seemingly our case organisation acts conform to Habermas' theory.

4. Forming a unified security culture – plausible or utopia?

According to our case, it seems that Habermas' theory of communicative act can be used to evaluate the process of forming a security culture. Another, rather interesting finding is that to form a unified security culture, at least the following things should be taken into account:

- The quantity of the group that determines the possibility for continuous communication.

- The unified set of values of the group members in the beginning of the culture creation process.
- The normative environment, both inside the group, and the influence of outside demands.
- Goals, which are set to perform plausible activity. In this case this is the foreseen end-state of the wholeness of the security.
- Resources, means and facts, which are available to perform plausible security enhancing activities.

We must bear in mind that culture is a structure, which exist to maintain patterns by the information called values. When again referring to figure 1., the way to information called values goes through norms. Norms are information, which determines the mutually understood code to perform collaboration successfully. To change values, the norms must be accepted and internalised first.

The third interesting point is that time must be taken into account. Unified structures in complex environments will not arise suddenly, they need a certain amount of time to manifest themselves. To develop a culture is always to cause more or less changes to personally understood values. The aim of forming a culture is to gain such structure, on which a solid base for all activities can be made. For this structure to be unified, values of individuals, organisation and customer should be as close to each other as possible. The more divergent they are, the longer the duration will be to unify them. In our case, the value base is rather unified in all these three parties thus making it somewhat easy to gain a unified security culture. This unity has been gained quicker than in ten years. If we take into account that no security clashes has happened in the case organisation, it could be stated that if strong security culture exists, a new member with a nearly unique value base compared to that of the organisation, will adapt to the organisation’s culture very quickly. It can therefore be stated that if the value base is unified, a unified security culture can be formed in less than a few years. This culture can be maintained, if motives and values of new employers are cleared and communicated in the recruiting process or at least in the very beginning of career. Figure 3. depicts the idea of time-divergent communication in developing security culture. As it is presented, to be able to effect on values (i.e. information concerning cultural structures), a long-term communication is demanded. On the other hand, if cultural structures can be formed, they will be somewhat stable for long periods of time. In that case, we can be rather

sure that this cultural unity will be well permanent for the foreseeable future, as well. Once formed, the culture will maintain.

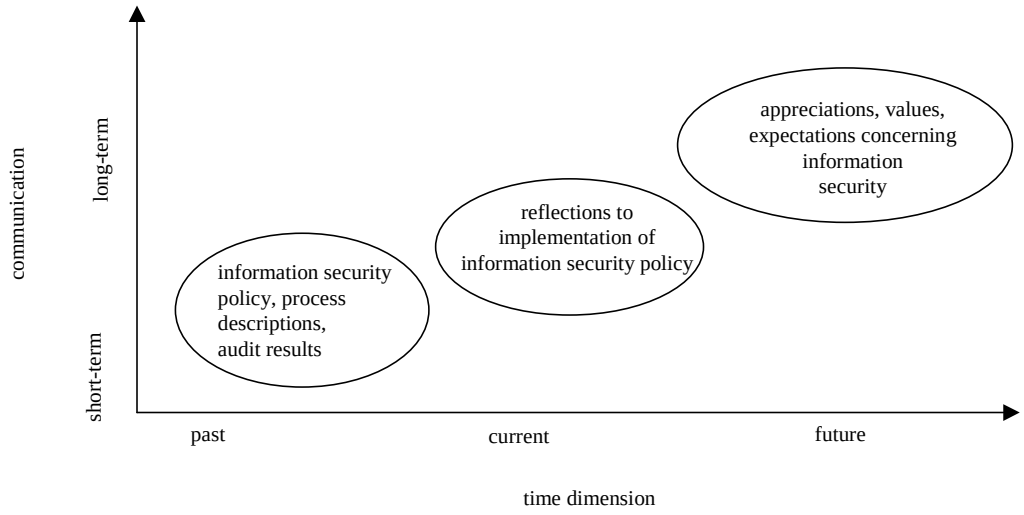

Fig. 3 Time-divergent communication for information security culture development in a value net, based on a general time-divergent communication model presented in (Helokunnas & Kuusisto 2003a). (Helokunnas & Kuusisto 2003b)

5. Conclusions

In this paper we introduced the theoretical frame about security culture based on Habermas' theory of communicative action. We approached the culture forming process via information concerning action orientation in the four-field of structural subsystems of institutions, policy, community and culture. Culture was determined as an activity of pattern maintenance via information concerning values. A great deal of energy is demanded to cause changes in cultural structures. Information concerning values is very abstracted and it is interpreted through the entire mental model. Values are somewhat established and the overall communication demanded to cause permanent changes takes a great deal of time.

Cultural changes cannot be made during a short period. Forming unite security culture is possible, but it will prerequisite at least either long period of time of possibility to exploit existing unity of values. In our case-unit the latter was realised. In this case the value-basis, i.e. the cultural structure, was rather uniting from the viewpoint of customer, organisation and employers. When so, it seems that unite security culture is somewhat easy to develop and maintain. This could be concluded from the basis of the theory we were using, as well.

From the basis of used theory verified by our case, we found five assumptions to be taken into account, when thinking the strategy to develop a unified security culture. These are:

1. Resources, which are set to perform security activities.
2. Security policy.
3. Commonly (global, national, customer, organisation) accepted norms.
4. The unity of values of all parties involved to security culture forming process.
5. The communication distance.

In this paper we focused on the fourth item. It seems that to gain unity in a cultural area, the normative layer must be well determined. The norms must be understood and accepted mutually. Acceptance will be easier if the value basis is commonly accepted, as well. So, norms and values are interacting, which is predicted by the theory, which we are using (see Figure 1.). Further on, it seems that the communicative distance is relevant. In our case, the unit was very cohesive and thus its communicative distance was short. People were working together and the change rate of personnel was low. All employees know each other and they understand each other rather well. This seems to have positive correlation, when forming a unified value basis. Anyhow, this was not examined in our study and we do not have validated results about that. We will leave this item open for further research.

References:

Anderson, R. (2001): *Security Engineering: A guide to Building Dependable Distributed Systems,* John Wiley & Co., USA.

Bell, W. (1998): *Foundations of Futures Studies. Vol II, Values, Objectivity, and the Good Society*, Transaction Publishers, New Brunswick (USA), London (UK).

Chia, P.A., Maynard, S.B., Ruighaver, A.B. (2002): Organisational Security Culture: Developing a Comprehensive research Model, in proc. of *IS ONE World Conference*, Las Vegas.

Dhillon, G. (1997): *Managing Information System Security*. Anthony Rowe Ltd., Chippenham, Wilthire.

Habermas, J. (1984): *The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society,* translated by Thomas McCarthy, Beacon Press, Boston.

Habermas, J. (1989): *The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason,* translated by Thomas McCarthy, Beacon Press, Boston.

Hofstede, G. (1984*)*: *Culture's Consequences: International Differences in Work-Relate Values*, Sage Publications, USA.

Helokunnas, T. and Kuusisto, R. (2003a): Strengthening Leading Situations via Time-divergent Communication Conducted in Ba, *Journal of eBusiness Review. Volume III, 2003*, pages 78 – 81.

Helokunnas, T and Kuusisto, R. (2003b): Information Security Culture in a Value Net, proc. of *2003 IEEE International Engineering Management Conference*, Albany, New York, pages 415 – 419

Jayaratha, N. (1994): *Understanding and Evaluating Methodologies: NIMSAD, a Systemic Framework*, McGraw and Hill, United Kingdom.

Kuusisto, R and Helokunnas, T. (2003): Ba, Communication and Time as Enablers of Leading, in proc. of *e-Business research Forum eBRF 2002*, Tampere, Finland 2003, pages 251 – 260.

Martins, A., Eloff, J. (2002): Information Security Culture, in *Security in the Information Society (ed. Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K.),* Kulwer Academic Publishers, USA, pages 203 – 214.

Parsons, T. (1951): *The Social System.* Glencoe.

von Solms, B. (2000), Information Security - The Third Wave? *Computers and Security* 19(7), pages 615-620.

Schein, E.H. (1992): *Organizational Culture and Leadership*. 2nd ed. Jossey-Bass, San Francisco, USA.

Schlinger, T., Teufel, S. (2000): Information Security Culture. The Socio-Cultural Dimension in Information Security Management, In proc. of *17th International Conference on Information Security (SEC 2002),* Kluwer Academic Publishers, USA.

Schneider, S., Barsoux, J-L. (1997): *Managing across cultures*, Prentice Hall, London, New York, Toronto, Sydney, Tokyo, Singapore, Madrid, Mexico City, Munich, Paris.

Tam, J.C. (2000): Personal Data Privacy in the Asia Pacific: A real Possibility, in proc. of *the 10th Conference of Computers, Freedom and Privacy,* ACM, Canada, pages 259 – 262.

Virtanen, T. (2002): *Four views on security*. Helsinki University of technology, Department of Computer Science and Engineering, Telecommunications Software and multimedia Laboratory, Otamedia Oy, Espoo.